INFORMATION SECURITY

SECURITY AWARENESS

APPLYING PRACTICAL SECURITY IN YOUR WORLD

Fifth Edition

Mark Ciampa

Security Awareness: Applying Practical Security In Your World

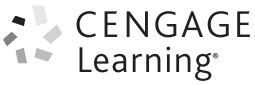
Security Awareness: Applying Practical Security In Your World

Fifth Edition

Mark Ciampa, Ph.D.

CENGAGE Learning®

Australia • Brazil • Mexico • Singapore • United Kingdom • United States



Security Awareness: Applying Practical Security In Your World, Fifth Edition

Mark Ciampa

SVP, GM Skills & Global Product Management: Dawn Gerrain

Product Director: Kathleen McMahon

Product Team Manager: Kristin McNary

Senior Director, Development: Marah Bellegarde

Product Development Manager: Leigh Hefferon

Senior Content Developer: Michelle Ruelos Cannistraci

Product Assistant: Abigail Pufpaff

Vice President, Marketing Services: Jennifer Ann Baker

Marketing Director: Michele McTighe

Senior Production Director: Wendy Troeger

Production Director: Patty Stephan

Senior Content Project Manager: Brooke Greenhouse

Managing Art Director: Jack Pendleton

Cover Image(s): © Alex Mit/Shutterstock.com

WCN: 02-200-203

Library of Congress Control Number: 2015957517

ISBN: 978-1-3055-0037-2

Cengage Learning
20 Channel Center Street
Boston, MA 02210
USA

Cengage Learning is a leading provider of customized learning solutions with employees residing in nearly 40 different countries and sales in more than 125 countries around the world. Find your local representative at **www.cengage.com**

Cengage Learning products are represented in Canada by Nelson Education, Ltd.

To learn more about Cengage Learning, visit **www.cengage.com**.

Purchase any of our products at your local college store or at our preferred online store **www.cengagebrain.com**.

Printed in the United States of America
Print Number: 01 Print Year: 2015

Brief Contents

Table of Contents

Preface

Security continues to be a major concern of virtually all computer users today. Consider the reasons why: attacks directed at point-of-sale (PoS) systems in retail stores resulted in over one billion records of consumers' payment card information being stolen in a single year, or an average of 2.8 million records stolen each day or 32 records every second.[i]

Almost one of three users in a survey said that either they or another household member had information from a payment card used at a store stolen by computer attackers during the last year, making this the most frequently experienced crime on a list of nine crimes.[ii] In a two-year period 91 percent of healthcare organizations reported at least one data breach, 39 percent reported two to five data breaches, and 40 percent had more than five data breaches. The total cost for healthcare data breaches is about $6 billion per year, with the average loss to each organization of $2,134,800.[iii] Security researchers recently demonstrated how easy it was for a car to be remotely controlled from a remote location 10 miles away, manipulating not only the car's air conditioning, radio, and windshield wipers, which the driver could not change, but also the acceleration and braking.[iv] This incident prompted the National Highway Traffic Safety Administration (NHTSA) to recall 1.4 million vehicles to patch this vulnerability, making it the first time that cars had been recalled due to security vulnerability.[v] It is no surprise that in a recent survey 69 percent of Americans report they frequently or occasionally worry about having their payment card information stolen by cyberattackers. This compares with 45 percent who worry about their home being burglarized and 7 percent who are concerned about being assaulted by a coworker.[vi]

Yet knowing how to make computer and mobile devices secure and keep them safe is still a puzzle to most users. What steps should you take to protect your computer, and which are the most important? How do you install software patches? Should you have antivirus software on your mobile device? What does a firewall do? What is a Trojan horse? How can you test your computer to be sure that it cannot be attacked through the Internet? Knowing how to keep a computer and mobile devices secure can be a daunting task.

This book provides you with the knowledge and tools you need to make your computer and related technology equipment—tablets, laptops, smartphones, and wireless networks—secure. *Security Awareness: Applying Practical Security in Your World, Fifth Edition*, presents a basic introduction to practical computer security for all users, from students to home users to business professionals. Security topics are introduced through a series of real-life user experiences, showing why computer security is necessary and providing the essential elements for making and keeping computers secure. Going beyond the concepts of computer security, you will gain practical skills on how to protect your computers and devices from increasingly sophisticated attacks.

Each chapter in the book contains Hands-On Projects that cover making computers secure, as well as how to use and configure security hardware and software. These projects are designed to make what you learn come alive through actually performing the tasks. Besides the Hands-On Projects, each chapter provides realistic security Case Projects that allow you to interact with other learners from around the world using the Information Security Community website that accompanies the textbook. Every chapter also includes review questions to reinforce your knowledge while helping you to apply practical security in your world.

Intended Audience

This book is intended to meet the needs of students and professionals who want to be able to protect their computers and technology devices from attacks. A basic working knowledge of computers is all that is required to use this book. The book's pedagogical features are designed to provide a truly interactive learning experience to help prepare you for the challenges of securing your technology. In addition to the information presented in the text, each chapter includes Hands-On Projects that guide you through implementing practical hardware, software, and network security step by step. Each chapter also contains case studies, requiring you to apply concepts presented in the chapter to achieve a successful solution.

Chapter Descriptions

Here is a summary of the topics covered in each chapter of this book:

- **Chapter 1, "Introduction to Security,"** begins by explaining the challenge of information security and why it is important. This chapter also introduces information security terminology, defines who the attackers are, and gives an overview of attacks and defenses.
- **Chapter 2, "Personal Security,"** examines attacks on passwords and the dangers of social engineering. It also covers identity theft and social networking risks, and provides information on personal security defenses to protect users from attacks.
- **Chapter 3, "Computer Security,"** explores attacks on computers that use different types of malware, such as viruses, worms, Trojans, and botnets. Chapter 3 also includes information on how to protect a computer by managing patches, examining firewalls, installing anti-malware software, and configuring personal firewalls. It also gives guidance on how to recover from an attack.

- **Chapter 4, "Internet Security,"** gives an overview of how the Internet works and the security risks that go along with using it. The chapter closes by exploring how to use the Internet securely.
- **Chapter 5, "Mobile Security,"** examines attacks that come through wireless networks, such as Wi-Fi and Bluetooth, along with attacks on mobile devices such as tablets, laptops, and smartphones. It also explores how networks and devices can be secured.
- **Chapter 6, "Privacy,"** explores the risks to private data along with privacy best practices. In addition, this chapter outlines the responsibilities of a business or organization to protect users' data.

Features

To aid you in fully understanding computer and network security, this book includes many features designed to enhance your learning experience.

- **Chapter Objectives.** Each chapter begins with a detailed list of the concepts to be mastered within that chapter. This list provides you with both a quick reference to the chapter's contents and a useful study aid.
- **Security in Your World.** Each chapter opens with a security-related vignette that introduces the chapter content and helps the reader to understand why these topics are important. These stories are continued throughout the chapter, providing additional information about real-life computer security.
- **Illustrations and Tables.** Numerous illustrations of security vulnerabilities, attacks, and defenses help you visualize security elements, theories, and concepts. In addition, the tables provide details and comparisons of practical and theoretical information.
- **Exceptional Security.** For those users who want to set the highest level of protection against cyberattacks, a series of practical suggestions is provided for going "above and beyond" a basic level of security.
- **Chapter Summaries.** Each chapter's text is followed by a summary of the concepts introduced in that chapter. These summaries provide a helpful way to review the ideas covered in each chapter.
- **Key Terms.** All of the terms in each chapter that were introduced with bold text are gathered in a Key Terms list at the end of the chapter, providing additional review and highlighting key concepts. Key term definitions are included in a Glossary at the end of the text.
- **Review Questions.** The end-of-chapter assessment begins with a set of review questions that reinforce the ideas introduced in each chapter. These questions help you evaluate and apply the material you have learned. Answering these questions will ensure that you have mastered the important concepts.
- **Hands-On Projects.** Although it is important to understand the concepts behind security, nothing can improve upon real-world experience. To this end, each chapter provides several Hands-On Projects aimed at providing you with practical security software and hardware implementation experience. These projects use the Windows 10 operating system, as well as software downloaded from the Internet.
- **Case Projects.** Located at the end of each chapter are two Case Projects. In these exercises, you implement the skills and knowledge gained in the chapter through real design and

implementation scenarios. Additional Case Projects, including a running case study that places you in the role of a problem solver, requiring you to apply concepts presented in the chapter, are available in the MindTap online learning environment.

New to This Edition

- Updated information on the latest security attacks and defenses
- Entirely new chapter on privacy
- New section in each chapter on exceptional security
- New Security in Your World vignettes in each chapter
- The latest information on and best practices for securing wireless networks and mobile devices (laptops, smartphones, and tablets)
- New material on cryptography and attacks using social engineering, and other topics
- New Hands-On Projects in each chapter covering some of the latest security software
- Updated Case Projects in each chapter
- Information Security Community Site activity in each chapter allows learners to interact with other learners and security professionals from around the world

Text and Graphic Conventions

Wherever appropriate, additional information and exercises have been added to this book to help you better understand the topic at hand. Icons throughout the text alert you to additional materials. The icons used in this textbook are described below.

The Note icon draws your attention to additional helpful material related to the subject being described.

Tips based on the author's experience provide extra information about how to attack a problem or what to do in real-world situations.

Each Hands-On activity in this book is preceded by the Hands-On icon and a description of the exercise that follows.

Case Project icons mark Case Projects, which are scenario-based assignments. In these case examples, you are asked to implement independently what you have learned.

Information Security Community Site

Stay secure with the Information Security Community Site! Connect with students, professors, and professionals from around the world, and stay on top of this ever-changing field.

Visit *www.community.cengage.com/infosec2* to:

- **Download** resources such as instructional videos and labs.
- **Ask** authors, professors, and students the questions that are on your mind in our Discussion Forums.
- **See** up-to-date news, videos, and articles.
- **Read** weekly blogs from author Mark Ciampa.
- **Listen** to podcasts on the latest Information Security topics.

Each chapter includes information on a current security topic and asks the learner to post their reactions and comments to the Information Security Community Site. This allows users from around the world to interact and learn from other users as well as with security professionals and researchers.

Instructor's Materials

Everything you need for your course is in one place! The following supplemental materials are available for use in a classroom setting. All the supplements available with this book are provided to the instructor online. Please visit *login.cengage.com* and log in to access instructor-specific resources on the Instructor's Companion Site.

Instructor's Manual. The Instructor's Manual that accompanies this textbook includes the following items: additional instructional material to assist in class preparation, including suggestions for lecture topics, tips on setting up a lab for the Hands-On Projects, and solutions to all end-of-chapter materials.

Cengage Learning Testing Powered by Cognero. This flexible, online system allows you to do the following:

- Author, edit, and manage test bank content from multiple Cengage Learning solutions.
- Create multiple test versions in an instant.
- Deliver tests from your LMS, your classroom, or wherever you want.

PowerPoint Presentations. This book comes with a set of Microsoft PowerPoint slides for each chapter. These slides are meant to be used as a teaching aid for classroom presentations, to be made available to students on the network for chapter review, or to be printed for classroom distribution. Instructors are also at liberty to add their own slides for other topics introduced.

Figure Files. All of the figures and tables in the book are reproduced. Similar to PowerPoint presentations, these are included as a teaching aid for classroom presentation, to make available to students for review, or to be printed for classroom distribution.

MindTap

MindTap for *Security Awareness: Applying Practical Security in Your World, Fifth Edition* is a fully online, highly personalized learning experience built upon Cengage Learning content. MindTap combines student learning tools—readings, multimedia, activities, and assessments—into a singular Learning Path that guides students through their course. Instructors personalize the experience by customizing authoritative Cengage Learning content and learning tools into the Learning Path that integrates into the MindTap framework seamlessly with Learning Management Systems.

Instant Access Code: (ISBN: 9781305946682)
Printed Access Code: (ISBN: 9781305946699)

To access additional course materials, go to *www.cengagebrain.com* and search for this book title periodically for more details.

About the Author

Mark Ciampa, Ph.D., Security+, is Associate Professor of Information Systems at Western Kentucky University in Bowling Green, Kentucky. Previously, he served as Associate Professor and Director of Academic Computing for 20 years at Volunteer State Community College in Gallatin, Tennessee. Dr. Ciampa has worked in the IT industry as a computer consultant for the U.S. Postal Service, the Tennessee Municipal Technical Advisory Service, and the University of Tennessee. He is also the author of many Cengage textbooks, including *Security+ Guide to Network Security Fundamentals, Fifth Edition*; *CWNA Guide to Wireless LANs, Third Edition*; *Guide to Wireless Communications*; and *Networking BASICS*. He holds a Ph.D. in technology management with a specialization in digital communication systems from Indiana State University.

Acknowledgments

A large team of dedicated professionals contributed to the creation of this book. I am honored to be part of such an outstanding group of professionals, and to everyone on the team I extend my sincere thanks. A special thanks goes to Product Manager Kristin McNary for her support and providing me the opportunity to work on this project. Thanks also to Associate Product Manager Amy Savino, Senior Content Developer Michelle Ruelos Cannistraci, Senior Content Project Manager Brooke Greenhouse, and to Serge Palladino, Technical Editor, as well as the excellent production and permissions teams at Cengage Learning.

Special recognition again goes to the very best developmental editor, Deb Kaufmann. As always, Deb was there to find all of my errors, watch every tiny detail of this project, answer my never-ending list of questions, and make very helpful suggestions. Without question, Deb is the developmental editor every author wishes for, and I was extremely grateful to have her on this project.

And finally, I want to thank my wonderful wife, Susan. What can I say? Once again her patience, support, and love gave me what I needed to finish this project. I could not have written the first word without her.

Dedication

To Braden, Mia, Abby, Gabe, Cora, and Will.

To the User

This book should be read in sequence, from beginning to end. However, each chapter is a self-contained unit, so after completing Chapter 1 the reader may elect to move to any subsequent chapter.

Hardware and Software Requirements

Following are the hardware and software requirements needed to perform the end-of-chapter Hands-On Projects.

- Microsoft Windows 10 (Projects may also be completed using Windows 8.1, 8, or 7 although the steps may slightly differ.)
- An Internet connection and web browser

Specialized Requirements

Whenever possible, the needs for specialized requirements were kept to a minimum. The following chapter features specialized hardware:

- Chapter 1: A USB flash drive

Free Downloadable Software Requirements

Free, downloadable software is required for the Hands-On Projects in the following chapters.

Chapter 1:

- Microsoft Safety Scanner
- Irongeek Thumbscrew

Chapter 2:

- KeePass Password Safe
- LastPass
- SuperGenPass

Chapter 3:

- EICAR AntiVirus Test File
- Macrium Reflect

Chapter 4:

- Qualys Browser Check
- Browzar Private Web Browser

Chapter 5:

- Xirrus Wi-Fi Monitor Inspector
- Prey Project

Chapter 6:

- OpenPuff Steganography
- Hashtab
- Criptext

References

i. "2014 Year of Mega Breaches & Identity Theft," *Breach Level Index*, accessed June 4, 2015. http://breachlevelindex.com/pdf/Breach-Level-Index-Annual-Report-2014.pdf.

ii. "Hacking Tops List of Crimes Americans Worry about Most," *Gallup*, accessed June 5, 2015. http://www.gallup.com/poll/178856/hacking-tops-list-crimes-americans-worry.aspx?utm_source=alert&utm_medium=email&utm_content=heading&utm_campaign=syndication.

iii. "Criminal Attacks: The New Leading Cause of Data Breach in Healthcare," Ponemon Institute, accessed June 4, 2015. http://www.ponemon.org/blog/criminal-attacks-the-new-leading-cause-of-data-breach-in-healthcare.

iv. Greenberg Andy, "Hackers Remotely Kill a Jeep on the Highway—With Me in It," *Wired*, July 21, 2015, accessed Aug. 6, 2015. http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

v. "Recalls and Defects," *NHTSA*, accessed Aug. 6, 2015. http://www.nhtsa.gov/Vehicle+Safety/Recalls+&+Defects.

vi. "Hacking Tops List of Crimes Americans Worry about Most," *Gallup*, accessed June 5, 2015. http://www.gallup.com/poll/178856/hacking-tops-list-crimes-americans-worry.aspx?utm_source=alert&utm_medium=email&utm_content=heading&utm_campaign=syndication.

chapter 1

Introduction to Security

After completing this chapter you should be able to do the following:

- Describe the challenges of securing information
- Define information security and explain why it is important
- Identify the types of attackers that are common today
- Describe attacks and defenses

Security in Your World

"Here's your latte," said Cora, as she set the two cups down on the table. Mia looked up from her phone. "Thanks. I promise I'll pay you back," she said. Mia and Cora had stopped at the coffee house between classes at the college they attended. "That's OK," said Cora. "But as I was paying for our drinks I noticed that the man in front of me pulled cash out of his billfold to pay for his coffee. Now when was the last time you saw someone here pay cash?"

Mia took a sip of her latte. "Well, it's not very often. How did you pay?" she asked. Cora sat down at the table. "I just tapped my phone on that black thing on the counter." Mia smiled. "So you used a contactless payment system by launching a mobile payment app on your smartphone and touching the reader." Cora laughed and said, "OK, if you say so." Mia was majoring in Computer Information Systems and wanted to go into the field of computer security, and she often tried to help Cora use the correct technical terminology. Mia set down her phone and said, "Well, maybe that man in front of you paid with cash because he was worried about security. In my Introduction to Computers class last week we read an article about how vulnerable these payment systems can be."

"Oh, there you go with security again," Cora said. "I think that is really overblown. I saw something online last week that said, "Millions of Internet Users Could Be at Risk" but I never heard of anyone who had a problem. And I've never been attacked, and you know how much time I spend online!" Mia grinned. "Oh, did you expect those millions of users to send you an email when they were attacked? Actually, you've already had some attacks targeted at you today." Cora looked puzzled. "Like what?"

Mia took another sip of her latte and then said to Cora, "Look at your school email account." As Cora took out her phone and looked at her emails Mia said, "Do you have a weird email from Tommaso?" Cora scrolled through her inbox and then stopped. "Yes, here it is. The only thing the email has is a link to a website I've never heard of. That's strange. Why did he send that to me? And how did you know about it?" Cora asked. Mia said, "I received the same one. Tommaso's email account has probably been compromised and it's sending out these spam emails to everyone in his address book, including you and me." "Well, he needs to have that antivirus software stuff on his computer," Cora said.

Mia picked up her phone again. "No, antivirus software doesn't stop everything. And look at this next email message: 'You have exceeded your email limit. All student email accounts need to be revalidated by clicking on the link below.' Of course, if you click on the links, you're bound to get infected, probably just like Tommaso. And did you see the email last week from the college that a database of personal records of over 100,000 students and alumni going back 5 years was stolen by attackers? Whoever did it may already have our names, addresses, Social Security numbers,

and even the financial data we used for our student loans. No antivirus software on your computer is going to stop that from happening."

Cora pushed her chair back in frustration. "Well, now I'm mad. Why can't they just stop these attacks? And how am I supposed to know what to do?"

Our world today is one in which everyone has been forced to continually protect themselves, their families, and their property from attacks by invisible foes. Bombings, random shootings, airplane hijackings, and other types of physical violence occur around the world with increasing frequency. To counteract this violence, new types of security defenses have been implemented. Passengers using public transportation are routinely screened before boarding. Fences are erected across borders. Telephone calls are monitored. These attacks and the security defenses against them have impacted virtually every element of our lives and they significantly affect how all of us live each and every day.

And these attacks are not just physical. Our computers and technology devices are also frequent targets of attacks. An endless stream of malicious attacks is directed at individuals, schools, businesses, and governments through desktop computers, laptops, smartphones, and tablets. Internet web servers must repel thousands of attacks every day. Identity theft using stolen electronic data has skyrocketed. An unprotected computer connected to the Internet can be infected within minutes. Terms like *phishing*, *rootkits*, *worms*, *zombies*, and *botnets*—virtually unheard of just a few years ago—are now part of our everyday security technology vocabulary.

Although all computer users have heard about attacks that can threaten the security of their devices—and many have already been victims of attacks—the overwhelming majority of users are unsure about how to actually make their devices secure. Ask yourself this question: If you were warned that a particularly nasty Internet attack was to be released within the next few hours, what would you do to protect your computer and the information on it? Install antivirus software? Download a patch? Turn on a firewall? Unplug your Internet connection? Or do nothing and hope for the best?

It is important for all computer users today to be knowledgeable about computer security and to know what steps to take to defend against attacks. Applying practical security in your world has never been more important than it is right now.

This chapter introduces you to computer security. It begins by examining the current challenges in computer security and why it is so difficult to achieve. It then describes information security in more detail and explores why it is important. Finally, the chapter looks at who is responsible for these attacks and outlines the steps to build a comprehensive security strategy.

Challenges of Securing Information

"Why can't we stop all these attacks?" is a question that is often heard. Although it may seem that there should be a straightforward and easy solution to preventing attacks and securing our computers, in reality there is no single simple solution. This can be seen through the different types of attacks that computer users face today as well as the difficulties in defending against these attacks.

Today's Attacks

Despite the fact that information security continues to rank as a high concern and tens of billions of dollars are spent annually on computer security, the number of successful attacks continues to increase. Information regarding recent attacks includes the following:

- Attacks directed at point-of-sale (PoS) systems in retail stores resulted in over 1.02 billion records of consumers' payment card information being stolen in a single year. This averages to 2.8 million records stolen each day or 32 records every second.[1] These malicious programs, called "memory-scrapers," steal a user's payment card numbers as soon as the card is swiped at the PoS. Because today's PoS terminals are specialized desktop or tablet computers, attackers are infecting these devices by sending emails to retailers that pretend to be from someone looking for a job, with the subject line as "Any Jobs?" or "My Resume." Attached to the email is a Microsoft Word file that pretends to be a resume and even says "Protected Document: This file is protected by Microsoft Office." Yet the file contains a malicious program that when opened will infect the PoS system.
- One of the main targets of attackers today is the healthcare industry. That is because healthcare records contain much more than just a patient's payment card number. These records contain medical information and financial information about the patient and family, which can then be used to steal their identities. In addition, stolen medical records can be used for billing fraud (charging medical treatments to the victim), for medical identity theft (pretending to be the victim to receive medical care), and even for purchasing drugs for resale. And because federal laws prohibit health plans from having annual or even lifetime dollar limits on most medical benefits, attackers can use stolen healthcare information to perform frauds that result in huge sums. An industry report revealed that in one year healthcare providers and payers reported a 60 percent increase in detected attacks, with financial losses from these attacks increasing 282 percent over the previous year.[2] Another report indicated that in a 24-month period 91 percent of healthcare organizations reported at least one breach, 39 percent reported two to five data breaches, and 40 percent had more than five data breaches. The total cost for healthcare data breaches is about $6 billion per year, with the average loss to each organization of $2,134,800.[3]
- Vulnerability in home wireless networking equipment was found in 90 products from 25 major manufacturers, which could allow attackers to launch their malicious software against any device connected to the home network. The vulnerable service that runs on the equipment cannot be disabled nor can the attacks coming from the Internet be blocked. While some manufacturers issued immediate fixes for their equipment, other manufacturers said that fixes would take several months to create and distribute to consumers. And some manufacturers said that their products have reached "end-of-life" and would not be patched.[4]
- A magazine reporter agreed to let two security researchers demonstrate how easy it was for a car to be remotely controlled. From a location ten miles away, the researchers manipulated the car's air conditioning, radio, and windshield wipers, which the driver could not change. As the driver pressed the accelerator while merging onto a crowded Interstate highway the car started slowing down with an 18-wheeler barreling down on him as the researchers continued to manipulate the car. The researchers even disabled the brakes so that the car ended up in a ditch.[5] This incident prompted the National Highway

Traffic Safety Administration (NHTSA) to recall 1.4 million vehicles to patch this vulnerability, making it the first time that cars had been recalled due to a security vulnerability.[6]

- It has been speculated for several years that someone could manipulate aircraft while in flight because the systems that control the aircraft are not properly protected. According to the FBI, a security researcher may have actually done that. On a flight between Chicago and Syracuse a researcher tweeted that he was probing the aircraft systems of his flight. The airlines' Cyber Security Intelligence Department, which monitors social media, saw the tweet and alerted the FBI. According to the FBI, a special agent later examined the first-class cabin seat where the researcher was seated and found that he had tampered with the Seat Electronic Box (SEB), which is located under some passenger seats. This allowed him to connect his laptop to the in-flight entertainment (IFE) system via the SEB. Once the researcher accessed the IFE he could then access other systems on the plane. The researcher claims that he was able to cause the airplane to climb after manipulating its software. The airline has now banned him from all of its flights.[7]
- Many cars today offer a Passive Keyless Entry and Start (PKES) system, which allows the driver to unlock the doors and start the car without having to take the key out of her pocket or purse. All a driver has to do is get close enough to the car for the wireless signal from their key fob to be detected by the car, and once detected the doors automatically unlock and the engine can be started by pushing a button on the dashboard. Recently a neighborhood in Los Angeles was experiencing a series of mysterious break-ins on cars that had PKES systems. One person, who happened to be a newspaper reporter, had his car entered three times but there was no evidence of forced entry. One day as the reporter watched his car from inside his house he saw a young girl ride up on her bicycle and then take out of her backpack a small black device. She then walked over and unlocked the car and climbed in. The owner ran outside and the girl quickly left. Evidently the girl used an inexpensive power amplifier: when she turned the amplifier on it increased to over 50 feet (15 meters) the distance that the car could search for the key fob. Although the key fob was sitting on the kitchen counter inside the reporter's house, the car was still able to detect it and was fooled into thinking that the driver was approaching the car.[8] The cost of the amplifier is as little as $17. Car owners who want to protect themselves from this attack are being told to put their keys in their freezer, which will stop an amplified signal from reaching the key.
- A sample set of tens of thousands of malicious files were scanned by the four most commonly deployed antivirus products. Within the first hour the antivirus products only identified 30 percent of the malicious software. It took 24 hours before these products correctly identified 66 percent of the infected files as malicious, and after seven days the accumulated total was 72 percent. However, it took more than six months for the four antivirus products to correctly identify and protect all of the malicious files. Based on the average number of infections being distributed by attackers this means that these antivirus products would have missed 796 malicious files each day.[9]
- The iconic entertainer Madonna was forced to quickly move up for immediate purchase the release of six tracks from one of her upcoming albums, although the album was not scheduled to appear for another three months. This emergency release was due to the fact that 13 prerelease recordings, which was probably the entire album, were stolen and leaked onto the Internet. In addition, previously unpublished photos were also taken and posted without permission. Madonna stated that in order to combat future leaks her content will no longer be placed on any devices that are connected to a

network or the Internet. Instead, hard drives containing music will be hand-carried to recipients. Madonna went on to say that at any future photo or video recordings everyone involved will be required to leave their cell phones checked at the door.[10]

- In a recent survey 69 percent of Americans report they frequently or occasionally worry about having their payment card information stolen by cyberattackers. This compares with 45 percent who worry about their home being burglarized and 7 percent who are concerned about being assaulted by a coworker. Americans between the ages of 30 and 64 worry about this more than younger and older Americans do. And almost one out of three said that either they or another household member had information from a payment card used at a store stolen by computer attackers during the last year, making this the most frequently experienced crime on a list of nine crimes.[11]
- Despite the fact that some Apple computer users may feel that their devices are more secure than those from other manufacturers, vulnerabilities in Apple devices continue to be exposed and manipulated by attackers. Recently a critical vulnerability on Apple computers was found based on a flawed energy conservation implementation that left protections unlocked on the affected Macs after they woke up from sleep mode. This vulnerability was rated as critical since it can provide an attacker with persistent access to a computer even if a user completely wiped her hard drive clean and reinstalled the operating system. All but the latest models of Apple Mac computers are affected by this vulnerability.[12]
- The number of security breaches that expose users' digital data to attackers continues to rise. From January 2005 through July 2015, over 853 million electronic data records in the United States were breached, exposing to attackers a range of personal electronic data, such as address, Social Security numbers, health records, and credit card numbers.[13] Table 1-1 lists some of the security breaches that occurred during only a one-month period, according to the Privacy Rights Clearinghouse.[14]

Organization	Description of security breach	Number of identities exposed
Office of Personnel Management	Current and former federal employees exposed employees' job assignments, performance, and training, and may have exposed Social Security information and/or financial information.	4,000,000
CareFirst BlueCross BlueShield	The breach of a single database exposed names, birth dates, email addresses, and insurance identification numbers.	1,100,000
Penn State's College of Engineering	In two different intrusions attackers accessed "sensitive data" of all College of Engineering students, faculty, and staff.	18,000
Salley Beauty	"Unusual activity of payment cards at some stores" followed a similar attack 60 days before in which information on over 25,000 customer payment cards was stolen.	Unknown
AT&T	In three separate incidents employees accessed customer names and Social Security numbers, which were then sold to outsiders who used that information to unlock stolen cell phones.	280,000
Anthem BlueCross BlueShield	Names, birthdays, medical IDs, Social Security numbers, street addresses, email addresses, employment and income information were stolen in an attack that may have gone undetected for ten months.	80,000,000

Table 1-1 Selected security breaches involving personal information in a one-month period

Difficulties in Defending against Attacks

The challenge of keeping computers secure has never been greater, not only because of the number of attacks but also because of the difficulties faced in defending against these attacks. These difficulties include the following:

- *Universally connected devices*. It is unthinkable today for any technology device—desktop computer, tablet, laptop, or smartphone—not to be connected to the Internet. Although this provides enormous benefits, it also makes it easy for an attacker halfway around the world to silently launch an attack against a connected device.
- *Increased speed of attacks*. With modern technology attackers can quickly scan millions of devices to find weaknesses and launch attacks with unprecedented speed. Today's attack tools initiate new attacks without any human participation, thus increasing the speed at which systems are attacked.
- *Greater sophistication of attacks*. Attacks are becoming more complex, making it more difficult to detect and defend against them. Attackers today use common Internet protocols and applications to perform attacks, making it more difficult to distinguish an attack from legitimate network traffic. Other attack tools vary their behavior so the same attack appears differently each time, further complicating detection.
- *Availability and simplicity of attack tools*. Whereas in the past an attacker needed to have an extensive technical knowledge of networks and computers as well as the ability to write a program to generate the attack, that is no longer the case. Today's software attack tools do not require any sophisticated knowledge on the part of the attacker. In fact, many of the tools, such as the Kali Linux interface shown in Figure 1-1, have a graphical user interface (GUI) that allows the user to easily select options from a menu. These tools are freely available or can be purchased from other attackers at a surprisingly low cost.
- *Faster detection of vulnerabilities*. Weakness in hardware and software can be more quickly uncovered and exploited with new software tools and techniques.
- *Delays in security updating*. Hardware and software vendors are overwhelmed trying to keep pace with updating their products against attacks. One antivirus software security institute receives more than 390,000 submissions of potential malware *each day*.[15] At this rate the antivirus vendors would have to create and distribute updates *every few seconds* to keep users fully protected. This delay in distributing security updates adds to the difficulties in defending against attacks.
- *Weak security updates distribution*. While vendors of mainstream products, such as Microsoft, Apple, and Adobe, have a system for notifying users of security updates for many of their products and distributing them on a regular basis, few other software vendors have invested in these costly distribution systems. Users are generally unaware that a security update even exists for a product because there is no reliable means for the vendor to alert the user. Also, these vendors often do not create small security updates that "patch" the existing software, but instead they fix the problem in an entirely new version of the software—and then require the user to pay for the updated version that contains the patch.

Figure 1-1 Menu of attack tools

Source: Kali Linux

Vendors of smartphone operating systems are particularly well known for not providing security updates on a timely basis, if at all. Most vendors and wireless carriers do not attempt to provide users with significant updates (such as from version 5.6 to 5.7), instead hoping that users will purchase an entirely new smartphone—and service contract—to have the latest and most secure device.

- *Distributed attacks*. Attackers can use hundreds of thousands of computers under their control in an attack against a single server or network. This "many against one" approach makes it virtually impossible to stop an attack by identifying and blocking a single source.
- *User confusion*. Increasingly, users are called upon to make difficult security decisions regarding their computer systems, sometimes with little or no information to guide them. It is not uncommon for a user to be asked security questions such as *Do you want to view only the content that was delivered securely?* or *Is it safe to quarantine this attachment?* or *Do you want to install this extension?* With little or no direction, users are inclined to provide answers to questions without understanding the security risks. In addition, popular information that is circulated about security through consumer news outlets or websites is often inaccurate or misleading, resulting in even more user confusion.

Table 1-2 summarizes the reasons why it is difficult to defend against today's attacks.

Reason	Description
Universally connected devices	Attackers from anywhere in the world can attack.
Increased speed of attacks	Attackers can launch attacks against millions of computers within minutes.
Greater sophistication of attacks	Attack tools vary their behavior so the same attack appears differently each time.
Availability and simplicity of attack tools	Attacks are no longer limited to highly skilled attackers.
Faster detection of vulnerabilities	Attackers can discover security holes in hardware or software more quickly.
Delays in security updating	Vendors are overwhelmed trying to keep pace updating their products against the latest attacks.
Weak security update distribution	Many software products lack a means to distribute security updates in a timely fashion.
Distributed attacks	Attackers use thousands of computers in an attack against a single computer or network.
User confusion	Users are required to make difficult security decisions with little or no instruction.

Table 1-2 Difficulties in defending against attacks

Security in Your World

As she waited for her class to start, Cora turned around to talk with her friend Abby about the conversation she had earlier with Mia. Cora said, "You read about this security stuff all the time, but I don't have a clue what they're talking about. It's like they're talking over my head about 'vulnerabilities' and 'threats.' " Abby nodded her head. "I know what you mean." Then she continued, "But who would want to break into our computers or cell phones? And so what if they did? What's the worst thing that can happen? They would read our email and texts? Let them! Really, what do we have that somebody would want?"

Cora opened her book as her instructor walked into the room. "But Mia said that there are all sorts of bad things that can happen if you're attacked." "Like what?" asked Abby skeptically. "Remember yesterday when you said that you went online and bought that birthday present for your brother and used your credit card number?" Cora asked. "Mia said that an attacker online could steal your credit card number and then use it to charge things to your account." Abby paused. She remembered that her Uncle Greg had his credit card number stolen earlier this year and had thousands of dollars charged on it. "And what if an attacker got into your computer and just erased everything? Think of all those photos you have stored on your computer. You wouldn't want to lose them." "Well, OK," said Abby.

(continues)

"And," Mia continued, "Remember when my brother Gabe got a virus or something on his computer and it wouldn't work right? He couldn't even use it. That was right before the end of the semester, and he had all of those papers he had written stored on the computer but he couldn't get to them. He had to stay up all night for several days to rewrite them. He was really mad and barely passed his literature class because of that." Abby turned off her cell phone's ringer as the instructor started class. "I do remember you talking about that. What else did Mia say these attackers could do?"

What Is Information Security?

Before it is possible to defend against attacks, it is necessary to understand exactly what security is and how it relates to information security. Also knowing the terminology used can be helpful when creating defenses for computers. Understanding the importance of information security is also critical.

Understanding Security

A search of the Internet to define the word *security* will result in a variety of definitions. Sometimes security is defined as *the state of being free from danger*, while at other times security is said to be *the protection of property*. And another interpretation of security is *the degree of resistance from harm*. The difference in these definitions actually hinges upon whether the focus is on the *process* (how to achieve security) or the *goal* (what it means to have security). In reality security is both: it is the goal to be free from danger as well as the process that achieves that freedom.

Yet because complete security can never be fully achieved, most often security is viewed as a process. In this light security may be defined as *the necessary steps to protect a person or property from harm*. This harm may come from one of two sources: either from a direct action that is intended to inflict damage or from an indirect and unintentional action. Consider a typical house: it is necessary to provide security for the house and its inhabitants from these two different sources. For example, the house and its occupants must be secure from the direct attack of a criminal who wants to inflict bodily harm to someone inside or a burglar who wants to steal a television. This security may be provided by locked doors, a fence, or a strong police presence. In addition, the house must also be protected from indirect acts that are not exclusively directed against it. That is, the house needs to be protected from a hurricane (by being built with strong materials and installing hurricane shutters) or a storm surge (by being built off the ground).

Security usually includes both preventive measures and rapid response. An individual who wants to be secure would take the preventive measures of keeping the doors to the house locked and leaving outside lights turned on at night. An example of a rapid response could include the homeowner programming *911* into his phone so that if anything suspicious begins to occur around the house an emergency call can be made quickly to the police.

It is also important to understand the relationship between *security* and *convenience*. As security is increased, convenience is often decreased. That is, the more secure something is, the less convenient it may become to use (security is said to be "inversely proportional" to convenience). This is illustrated in Figure 1-2. Consider again a typical house. A homeowner might install an automated alarm system that requires a code to be entered on a keypad within 30 seconds of entering the house. Although the alarm system makes the house more secure, it is less convenient than just walking into the house. Thus, security may be understood as *sacrificing convenience for safety*. Another way to think of security is *giving up short-term comfort for long-term protection*. In any case, security usually requires forgoing convenience to achieve a greater level of safety or protection.

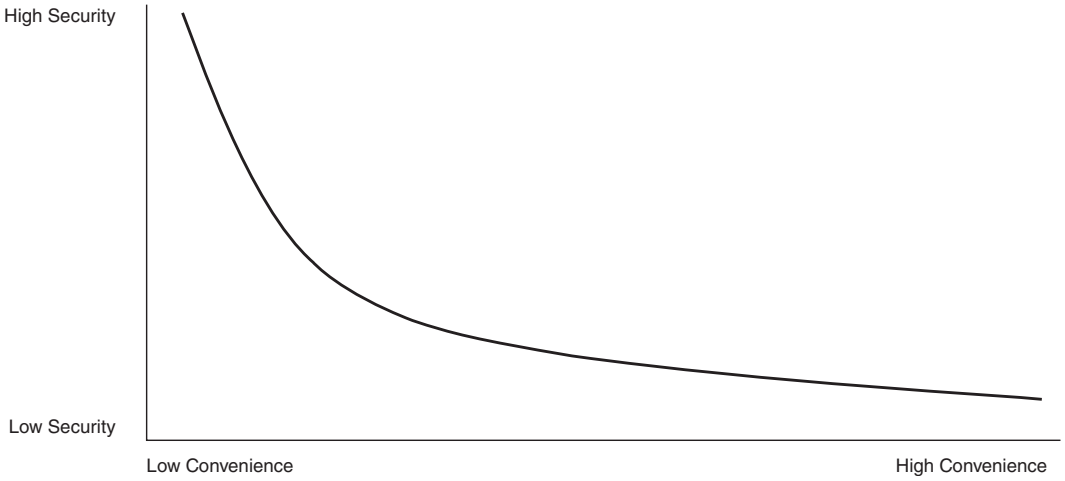


Figure 1-2 Relationship of security to convenience

Defining Information Security

The term **information security** is frequently used to describe the tasks of securing information that is in a digital format. This digital information is manipulated by a microprocessor (such as on a personal computer), stored on a storage device (like a hard drive or USB flash drive), and transmitted over a network (such as a local area network or the Internet).

Just as security can be viewed as both a goal and a process, the same is true with information security. Information security can be best understood by examining its goals and the process of how it is accomplished. Together these can help create a solid definition of information security.

Information security cannot completely prevent successful attacks or guarantee that a system is totally secure, just as the security measures taken for a house can never guarantee complete safety from a burglar or a hurricane. The intention of information security is to ensure that protective measures are properly implemented to ward off attacks and provide protection to the highest possible degree. It also should prevent the total collapse of the system when a successful attack does occur. Thus, information security is first *protection*.

Information security should not be viewed as a war to be won or lost. Just as crime such as burglary can never be completely eradicated, neither can attacks against technology devices. The goal is not a complete victory but instead maintaining equilibrium: as attackers take advantage of a weakness in a defense, defenders must respond with an improved defense. Information security is an endless cycle between attacker and defender.

Second, information security is intended to protect *information* that provides value to people and organizations. There are three protections that must be extended over information: confidentiality, integrity, and availability, sometimes called the *CIA triad*:

1. *Confidentiality*. It is important that only approved individuals are able to access important information. For example, the credit card number used to make an online purchase must be kept secure and not made available to other parties. **Confidentiality** ensures that only authorized parties can view the information. Providing confidentiality can involve several different security tools, ranging from software to "scramble" the credit card number stored on the web server to door locks to prevent access to those servers.
2. *Integrity*. **Integrity** ensures that the information is correct and no unauthorized person or malicious software has altered the data. In the example of the online purchase, an attacker who could change the amount of a purchase from $10,000.00 to $1.00 would violate the integrity of the information.
3. *Availability*. Information has value if the authorized parties who are assured of its integrity can access the information. **Availability** ensures that data is accessible to authorized users (and that the information is not "locked up" so tight that they cannot access it). It also means that attackers have not performed an attack so that the data cannot be reached. In this example the total number of items ordered as the result of an online purchase must be made available to an employee in a warehouse so that the correct items can be shipped to the customer.

In addition to the CIA triad, another set of protections must be implemented to secure information. These are authentication, authorization, and accounting—or *AAA*:

1. *Authentication*. **Authentication** ensures that the individual is who she claims to be (the authentic or genuine person) and not an imposter. A person accessing the web server that contains a user's credit card number must prove that she is indeed who she claims to be and not a fraudulent attacker. One way in which authentication can be performed is by the person providing a password that only she knows.
2. *Authorization*. **Authorization** is providing permission or approval to specific technology resources. After a person has provided authentication she may have the authority to access the credit card number or enter a room that contains the web server, provided she has been given prior authorization.
3. *Accounting*. **Accounting** provides tracking ("audit trail") of events. This may include a record of who accessed the web server, from what location, and at what specific time.

Yet how is the information protected? Because this information is stored on computer hardware, manipulated by software, and transmitted by communications, each of these areas must be sheltered. The third objective of information security is to protect the integrity,

confidentiality, and availability of information *on the devices that store, manipulate, and transmit the information.*

Information security is achieved through a process that is a combination of three entities. As shown in Figure 1-3 and Table 1-3, information and the hardware, software, and communications are protected in three layers: products, people, and policies and procedures. These three layers interact with each other: procedures enable people to understand how to use products to protect information.

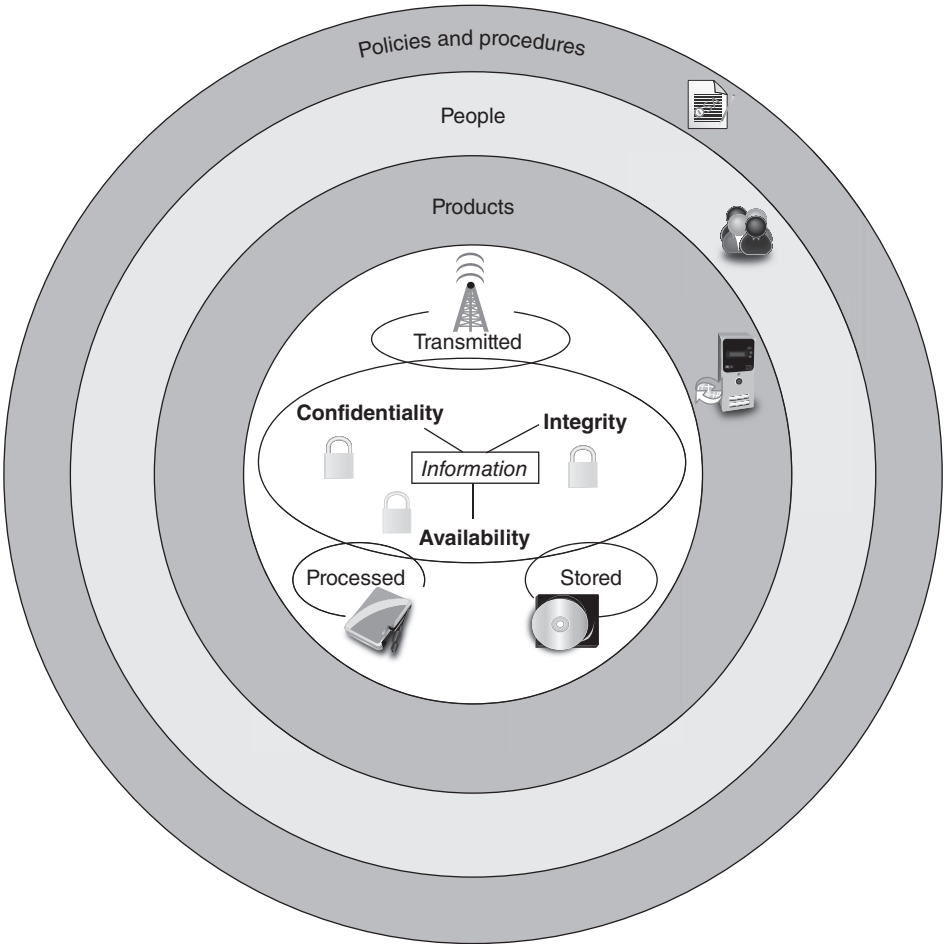


Figure 1-3 Information security layers

Layer	Description
Products	Forms the security around the data. May be as basic as door locks or as complicated as network security equipment.
People	Those who implement and properly use security products to protect data.
Policies and procedures	Plans and policies established by an organization to ensure that people correctly use the products.

Table 1-3 Information security layers

A comprehensive definition of information security involves both the goals and process. Information security may be defined as *that which protects the integrity, confidentiality, and availability of information on the devices that store, manipulate, and transmit the information through products, people, and procedures.*

Information Security Terminology

As with many advanced subjects, information security has its own set of terminology. The following scenario helps to illustrate information security terms and how they are used.

Suppose that Ellie wants to purchase a new motorized Italian scooter to ride from her apartment to school and work. However, because several scooters have been stolen near her apartment she is concerned about its protection. Although she parks the scooter in the gated parking lot in front of her apartment, a hole in the fence surrounding the apartment complex makes it possible for someone to access the parking lot without restriction. Ellie's scooter and the threat to it are illustrated in Figure 1-4.

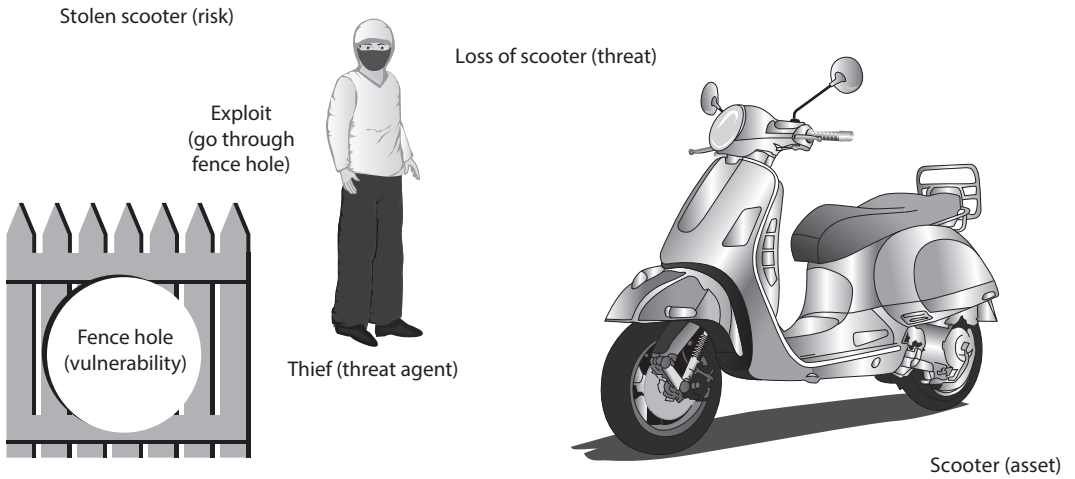


Figure 1-4 Information security components analogy

Ellie's new scooter is an **asset**, which is defined as an item that has value. What Ellie is trying to protect her scooter from is a **threat**, which is a type of action that has the potential to cause harm. Information security threats are events or actions that represent a danger to information assets. A threat by itself does not mean that security has been compromised; rather, it simply means that the potential for creating a loss is real.

A **threat agent** is a person or element that has the power to carry out a threat. For Ellie the threat agent is a thief. In information security, a threat agent could be a person attempting to break into a secure computer network. It could also be a force of nature such as a hurricane that could destroy computer equipment and thus destroy information, or it could be malicious software that attacks the computer network.

Ellie wants to protect her scooter and is concerned about a hole in the fencing around her apartment. The hole in the fencing is a **vulnerability**, which is a flaw or weakness that allows a threat agent to bypass security. An example of a vulnerability that information security must deal with is a software defect in an operating system that allows an unauthorized user to gain control of a computer without the user's knowledge or permission.

If a thief can get to Ellie's scooter because of the hole in the fence, then that thief is taking advantage of the vulnerability. This is known as exploiting the vulnerability through a **threat vector**, or the means by which an attack can occur. An attacker, knowing that a flaw in a web server's operating system has not been patched, may use a threat vector (exploiting the vulnerability) to steal user passwords.

Ellie must make a decision: what is the probability (**threat likelihood**) that the threat will come to fruition and her scooter stolen? This can be understood in terms of risk. A **risk** is a situation that involves exposure to some type of danger. There are different options that Ellie could take regarding the risk of her scooter being stolen. Ellie could decide based on the risk of the scooter being stolen that she will not purchase the new scooter (*risk avoidance*). Or she could accept the risk and buy the new scooter, knowing there is the chance of it being stolen by a thief entering through a hole in the fence (*risk acceptance*). She might complain to the apartment manager about the hole in the fence in order to have it repaired and make risk less serious (*risk mitigation*) or ask the manager to post signs that said "Trespassers will be punished to the full extent of the law" (*risk deterrence*). What Ellie is most likely to do is purchase insurance so that the insurance company absorbs the loss and pays her if the scooter is stolen, in essence making someone else responsible (*risk transference*).

Table 1-4 summarizes these information security terms.

Term	Example in Ellie's scenario	Example in information security
Asset	Scooter	Employee database
Threat	Steal scooter	Steal data
Threat agent	Thief	Attacker, hurricane
Vulnerability	Hole in fence	Software defect
Threat vector	Climb through hole in fence	Access web server passwords through software flaw
Threat likelihood	Probability of scooter stolen	Likelihood of virus infection
Risk	Not purchase scooter	Not install wireless network

Table 1-4 Information security terminology

Understanding the Importance of Information Security

Information security is important to individuals as well as organizations. That is because information security can be helpful in preventing data theft, thwarting identity theft, avoiding the legal consequences of not securing information, maintaining productivity, and foiling cyberterrorism.

Preventing Data Theft *Security* is most often associated with theft prevention: Ellie could park her scooter in a locked garage in order to prevent it from being stolen. The same is true with information security: preventing data from being stolen is often cited as a primary objective of information security. For a business it is necessary to guard against data theft. Attackers are eager to steal proprietary business information, such as research for a new product or a list of customers.

Individuals as well are often the targets of data thievery. A type of personal data that is a prime target of attackers is payment card numbers, such as debit cards, credit cards, and gift cards. These stolen numbers can be sold on the black market to be used to purchase thousands of dollars of merchandise online—without having the actual card—before the victim or bank is even aware the number has been stolen. Some of the common techniques used by payment card thieves include:

- Thieves determine if a stolen card number is still active by making a small purchase, which is unlikely to generate the attention of the user or the bank that issued the card.
- Some black-market sellers will provide a guarantee that the stolen card numbers will remain active for a specific period of time or for the purchase of a minimum amount of merchandise before the card number is revoked.
- Black-market sellers will often monitor how their customers use the stolen cards in order to ensure they do not generate too much attention and thus risk being discovered, which would then prevent other customers who have purchased similar cards from being able to make purchases.
- Stolen card numbers that also include personal information such as the birth date and Social Security number of the card holder are worth more than just the card number itself. That is because thieves can use this information to uncover other personal information about the victim and thus be in a better position to answer security challenge questions that might be asked by the bank if a large purchase is being made.

Thwarting Identity Theft **Identity theft** involves stealing another person's personal information, such as a Social Security number, and then using the information to impersonate the victim, generally for financial gain. The thieves often create new bank or credit card accounts under the victim's name and then large purchases are charged to these accounts, leaving the victim responsible for the debts and ruining her credit rating.

In some instances, thieves have bought cars and even houses by taking out loans in someone else's name.

One rapidly growing area of identity theft involves identity thieves filing fictitious income tax returns with the U.S. Internal Revenue Service (IRS) in order to receive the victim's tax refund. According to the IRS, each year over $6 billion in refund checks are sent to identity thieves who filed fraudulent tax returns. However, enforcement still remains a problem.[16]

Montgomery, Alabama, has the second-highest number of identity thefts in the nation. This may be due to the fact that the city is home to a large pool of what are called "perfect victims" who do not routinely file tax returns, notably the elderly in nursing homes and prisoners. There have also been instances of identity thieves filing fake tax returns while still using the victims' actual mailing addresses, but then bribing postal workers to intercept the refund checks before they are delivered. One postal employee in Montgomery was convicted of stealing over 100 refund envelopes sent to addresses along his route.[17]

Avoiding Legal Consequences Several federal and state laws have been enacted to protect the privacy of electronic data. Businesses that fail to protect data they possess may face serious financial penalties. Some of these laws include the following:

- *The Health Insurance Portability and Accountability Act of 1996 (HIPAA)*. Under the **Health Insurance Portability and Accountability Act (HIPAA)**, healthcare enterprises must guard protected healthcare information and implement policies and procedures to safeguard it, whether it be in paper or electronic format. Those who wrongfully disclose individually identifiable health information can be fined up to $50,000 for each violation up to a maximum of $1.5 million per calendar year and sentenced up to 10 years in prison.

HIPAA regulations have been expanded to include all third-party "business associate" organizations that handle protected healthcare information. Business associates are defined as any subcontractor that creates, receives, maintains, or transmits protected health information on behalf of a covered HIPAA entity. These associates must now comply with the same HIPAA security and privacy procedures.

- *The Sarbanes–Oxley Act of 2002 (Sarbox)*. As a reaction to a rash of corporate fraud, the **Sarbanes–Oxley Act (Sarbox)** is an attempt to fight corporate corruption. Sarbox covers the corporate officers, auditors, and attorneys of publicly traded companies. Stringent reporting requirements and internal controls on electronic financial reporting systems are required. Corporate officers who willfully and knowingly certify a false financial report can be fined up to $5 million and serve 20 years in prison.
- *The Gramm–Leach–Bliley Act (GLBA)*. Like HIPAA, the **Gramm–Leach–Bliley Act (GLBA)** passed in 1999 protects private data. GLBA requires banks and financial institutions to alert customers of their policies and practices in disclosing customer information. All electronic and paper data containing personally identifiable financial information must be protected. The penalty for noncompliance for a class of individuals is up to $500,000.
- *Payment Card Industry Data Security Standard (PCI DSS)*. The **Payment Card Industry Data Security Standard (PCI DSS)** is a set of security standards that all companies that process, store, or transmit credit card information must follow. PCI DSS applies to any organization or merchant, regardless of its size or number of card transactions, that processes transactions either online or in person. The maximum penalty for not complying is $100,000 per month.
- *State notification and security laws*. Since the passage of California's Database Security Breach Notification Act in 2003, all other states (with the exception of New Mexico

and South Dakota) have passed similar notification laws. These laws typically require businesses to inform residents within a specific period of time (typically 48 hours) if a breach of personal information has or is believed to have occurred. In addition several states have recently strengthened their own security laws. For example, Connecticut requires any organization doing business in the state to "scramble" all sensitive personal data that is being transmitted over a public Internet connection or stored on portable devices like a USB flash drive, and companies must notify any potential victims of a data breach within 90 days of the attack and offer at least one year of identity theft prevention services. Oregon's law includes protection of an individual's healthcare information while New Hampshire requires the state's education department to notify students and teachers if their personal data was possibly stolen.

The penalties for violating these laws can be sizeable. Businesses must make every effort to keep electronic data secure from hostile outside forces to ensure compliance with these laws and avoid serious legal consequences.

Maintaining Productivity Cleaning up after an attack diverts time, money, and other resources away from normal activities. Users who are victims of a successful attack may spend days restoring their computers to the state prior to the attack, or they may have to pay a technology professional to complete the task. During this time the computer is unavailable and personal productivity suffers.

Employees of an organization likewise are impacted due to an attack that renders their device useless. These workers cannot be productive and complete important tasks during or after an attack because computers and networks cannot function properly. Table 1-5 provides a sample estimate of the lost wages and productivity during an attack and the subsequent cleanup.

Number of total employees	Average hourly salary	Number of employees to combat attack	Hours required to stop attack and clean up	Total lost salaries	Total lost hours of productivity
100	$25	1	48	$4,066	81
250	$25	3	72	$17,050	300
500	$30	5	80	$28,333	483
1,000	$30	10	96	$220,000	1293

Table 1-5 Cost of attacks

Foiling Cyberterrorism The FBI defines **cyberterrorism** as any "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against noncombatant targets by subnational groups or clandestine agents."[18] Unlike an attack that is designed to steal information or erase a user's hard disk drive, cyberterrorism attacks are intended to cause panic or provoke violence among citizens. Attacks are directed at targets such as the banking industry, military installations, power plants, air traffic control centers, and water systems. These are desirable targets because they can significantly disrupt the normal activities of a large population. For

example, disabling an electrical power plant could cripple businesses, homes, transportation services, and communications over a wide area. Yet one of the challenges in combating cyberterrorism is that many of the prime targets are not owned and managed by the federal government. Because these are not centrally controlled, it is difficult to coordinate and maintain security.

The Department of Homeland Security has identified 7,200 key industrial control systems that are part of the critical infrastructure and are directly connected to the Internet, making them vulnerable to cyberterrorism attacks. In one year a 52 percent increase in attacks resulted in 198 directed attacks against these systems, resulting in several successful break-ins.[19]

Security in Your World

Mia set her glass down and listened to her friends while they ate lunch in the cafeteria. The school had recently been the victim of another hoax in which students and faculty had received an email from an attacker pretending to be from the school's IT department. The email asked the users to enter their username and password for verification. Because so many users had submitted their passwords the school decided to prevent anyone from logging in until new security procedures were implemented. Mia's psychology class was canceled because they could not use the computers in the lab.

"Teenagers," said Giulio, one of Mia's friends. "They're the ones who do these things. They have nothing better to do than write these programs that mess up somebody else's computer."

Esteban said, "I read somewhere that it's international terrorists who are behind all these attacks. They want to bring our country down so they're after our computers."

"I don't think so," said Li. "I'll bet it's the companies that sell computer security programs. They might write these attack programs so that people will have to buy their stuff."

Just then Professor Helba walked by their table. "Who do you think is behind these attacks?" Mia asked him. He smiled and said, "Teachers. They do it to cancel classes."

Who Are the Attackers?

In the past the term *hacker* referred to a person who used advanced computer skills to attack computers. However, that term did not accurately reflect the different motives and goals of the attackers. Instead, today more descriptive categories of attackers are used, including: cybercriminals, script kiddies, brokers, insiders, cyberterrorists, hactivists, and state-sponsored attackers.

Cybercriminals

The generic term **cybercriminals** is often used to describe individuals who launch attacks against other users and their computers (another generic word is simply *attackers*). However, strictly speaking cybercriminals are a loose network of attackers, identity thieves, and financial fraudsters who are highly motivated, less risk averse, well funded, and tenacious. Some security experts believe that many cybercriminals belong to organized gangs of young attackers, often clustered in Eastern European, Asian, and Third World regions. Cybercriminals often meet in hidden online "underground" forums to trade information, buy and sell stolen data and attacker tools, and even coordinate attacks. Table 1-6 describes how these forums are different from typical websites.

Name	Description	Example
Surface web	Anything that can be found and indexed by a search engine	Textbook publisher website
Deep web	Content that cannot be found by a search engine but only through a search dialog box on the site	State medical license database
Dark web	Information that has been intentionally hidden and cannot be accessed through a standard web browser	Attacker black market site

Table 1-6 Underground forums

Instead of attacking a computer to show off their technology skills (*fame*), cybercriminals have a more focused goal of financial gain (*fortune*): cybercriminals exploit vulnerabilities to steal information or launch attacks that can generate income. This difference makes the new attackers more dangerous and their attacks more threatening. These targeted attacks against financial networks and the theft of personal information are sometimes known as **cybercrime**.

Financial cybercrime is often divided into two categories. The first category focuses on individuals and businesses. Cybercriminals steal and use stolen data, credit card numbers, online financial account information, or Social Security numbers to profit from their victims or send millions of spam emails to peddle counterfeit drugs, pirated software, fake watches, and pornography.

The second category focuses on businesses and governments. Cybercriminals attempt to steal research on a new product from a business so that they can sell it to an unscrupulous foreign supplier who will then build an imitation model of the product to sell worldwide. This deprives the legitimate business of profits after investing hundreds of millions of dollars in product development, and because these foreign suppliers are in a different country they are beyond the reach of domestic enforcement agencies and courts. Governments are also the targets of cybercriminals: if the latest information on a new missile defense system can be stolen it can be sold—at a high price—to that government's enemies.

Some security experts maintain that East European cybercriminals are mostly focused on activities to steal money from individuals and businesses, whereas cybercriminals from East Asia are more interested in stealing data from governments or businesses. This results in different approaches to their attacks. East European cybercriminals tend to use custom-built, highly complex malware while East Asian attackers use off-the-shelf malware and simpler techniques. Also East European attackers work in small, tightly knit teams that directly profit from their attacks. East Asian cybercriminals usually are part of a larger group of attackers who work at the direction of large institutions from which they receive instructions and financial backing.

Script Kiddies

Script kiddies are younger individuals who want to attack computers, yet they lack the knowledge of computers and networks needed to do so. Script kiddies instead do their work by downloading automated attack software (scripts) from websites and using it to perform malicious acts. Figure 1-5 illustrates the skills needed for creating attacks. Over 40 percent of attacks require low or no skills and are frequently conducted by script kiddies.

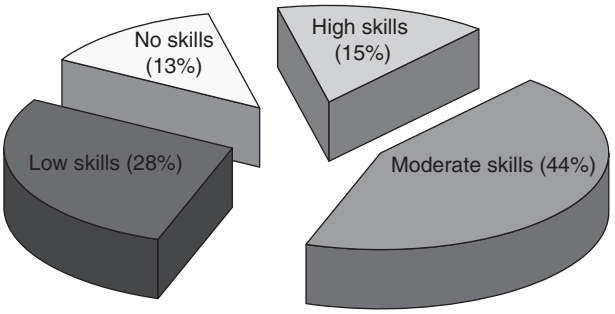


Figure 1-5 Skills needed for creating attacks

Today script kiddies can acquire entire **exploit kits** from other attackers to easily craft an attack. Script kiddies can either rent or purchase the kit from its authors and then specify various options to customize their attacks.

It is estimated that three out of every four Internet-based attacks originate from exploit kits.[20]

Brokers

In recent years several software vendors have started financially rewarding individuals who uncover vulnerabilities in their software and then privately report it back to the vendors so that the weaknesses can be addressed. Some vendors even sponsor annual competitive contests called "Bug Bounties" and handsomely pay those who can successfully attack their software in order to reveal vulnerabilities.

Google recently paid one security researcher $150,000 for uncovering a single bug.[21] In one year Facebook paid 321 researchers from 65 countries (India had the most submissions at 196 while the United States was third with 61) a total of $1.3 million for uncovering bugs, which enabled Facebook to then fix 61 high-severity vulnerabilities, twice as many as the previous year.[22]

However, other individuals who uncover vulnerabilities do not report it to the software vendor but instead sell them to the highest bidder. Known as **brokers**, these attackers sell their knowledge of a vulnerability to other attackers or even governments. These buyers are generally willing to pay a high price because this vulnerability is unknown to the software vendor

and thus is unlikely to be "patched" until after new attacks based on it are already widespread.

Insiders

Another serious threat to an organization actually comes from an unlikely source: its employees, contractors, and business partners, often called **insiders**. For example, a healthcare worker disgruntled over an upcoming job termination might illegally gather health records on celebrities and sell them to the media, or a securities trader who loses billions of dollars on bad stock bets could use her knowledge of the bank's computer security system to conceal the losses through fake transactions. In one study of 900 cases of business "data leakage," over 48 percent of the breaches were attributed to insiders who abused their right to access corporate information.[23] These attacks are harder to recognize because they come from within the organization yet may be more costly than attacks from the outside.

Most malicious insider attacks consist of the sabotage or theft of intellectual property. One study revealed that most cases of sabotage come from employees who have announced their resignation or have been formally reprimanded, demoted, or fired. When theft is involved, the offenders are usually salespeople, engineers, computer programmers, or scientists who actually believe that the accumulated data is owned by them and not the organization (most of these thefts occur within 30 days of the employee resigning). In some instances the employees are moving to a new job and want to take "their work" with them, while in other cases the employees have been bribed or pressured into stealing the data. In about 8 percent of the incidences of theft, employees have been pressured into stealing from their employer through blackmail or the threat of violence.[24]

In recent years insiders who worked either directly or indirectly for a government have stolen large volumes of sensitive information and then published it. The purpose is to alert its citizens of clandestine governmental actions and to pressure the government to change its policies.

Cyberterrorists

Many security experts fear that terrorists will turn their attacks to a nation's network and computer infrastructure to cause disruption and panic among citizens. Known as **cyberterrorists**, their motivation is ideological, attacking for the sake of their principles or beliefs. Cyberterrorists may be the attackers that are most feared, for it is almost impossible to predict when or where an attack may occur. Unlike cybercriminals who continuously probe systems or create attacks, cyberterrorists can be inactive for several years and then suddenly strike in a new way. Their targets may include a small group of computers or networks that can affect the largest number of users, such as the computers that control the electrical power grid of a state or region.

Hactivists

Another group motivated by ideology is **hactivists**. Unlike cyberterrorists who launch attacks against foreign nations to incite panic, hactivists (a combination of the words *hack* and *activism*) are generally not as well defined. Attacks by hactivists can involve breaking into a website and changing the contents on the site as a means of making a political statement against those who oppose their beliefs. In addition to attacks as a means of protest or to promote a

political agenda, other attacks can be retaliatory. For example, hactivists may disable the website belonging to a bank because that bank stopped accepting online payments that were deposited into accounts belonging to the hactivists.

State-Sponsored Attackers

Instead of using an army to march across the battlefield to strike an adversary, governments are using **state-sponsored attackers** for launching computer attacks against their foes. The foes may be foreign governments or even citizens of its own nation that the government considers hostile or threatening. A growing number of attacks today from state-sponsored attackers are directed toward businesses in foreign countries with the goal of causing financial harm or damage to the organization's reputation.

Many security researchers believe that state-sponsored attackers may be the most deadly of any attackers. That is because state-sponsored attackers are highly skilled and have enough government resources to breach almost any security defense. When an attacker motivated by fortune, like cybercriminals, finds that the target's defenses are too strong, the attacker simply moves on to another promising target with less-effective defenses. With state-sponsored attackers the target is very specific and the attackers keep working until they are successful, showing both deep resources and tenacity.

Table 1-7 lists several characteristics of these different types of attackers.

Attacker category	Objective	Typical target	Sample attack
Cybercriminals	Fortune over fame	Users, businesses, governments	Steal credit card information
Script kiddies	Thrills, notoriety	Businesses, users	Erase data
Brokers	Sell vulnerability to highest bidder	Any	Find vulnerability in operating system
Insiders	Retaliate against employer, shame government	Governments, businesses	Steal documents to publish sensitive information
Cyberterrorists	Cause disruption and panic	Businesses	Cripple computers that control water treatment
Hactivists	Right a perceived wrong against them	Governments, businesses	Disrupt financial website
State-sponsored attackers	Spy on citizens, disrupt foreign government	Users, governments	Read citizen's email messages

Table 1-7 Characteristics of attackers

Building a Comprehensive Security Strategy

What would a practical, comprehensive security strategy look like? There are four key elements to creating a practical security strategy: block attacks, update defenses, minimize losses, and stay alert. These elements are by no means new; these tactics go back to the days of

medieval castles in Europe and probably much earlier. Understanding these key elements as they were used during the Middle Ages helps bring them into focus for developing practical security today.

Block Attacks

The word *castle* comes from a Latin word meaning *fortress*, and most ancient castles served in this capacity. One of a castle's primary functions was to protect the king's family and citizens of the countryside in the event of an attack from an enemy. A castle was designed to block enemy attacks in two distinct ways. First, a castle was surrounded by a deep moat that was filled with water, which prevented the enemy from getting close to the castle. In addition, many castles had a high protective stone wall between the moat and the outer walls of the castle. The purpose of the moat and protective wall was to create a *security perimeter* around the castle: any attacker would have to get through the strong perimeter to get inside. This security perimeter was built and maintained by those tasked with protecting the castle

Effective information security follows this same model of blocking attacks by having a strong security perimeter. Usually, this security perimeter is part of the computer network to which a personal computer is attached, and in most settings, like a school or business, it is maintained by security professionals. If attacks are blocked by the network security perimeter, the attacker will be unable to reach the personal computer on which the data is stored. Security devices can be added to a computer network that will continually analyze traffic coming into the network from outside (such as email or webpages) and block unauthorized or malicious traffic.

In addition to perimeter security, most castles provided *local security*. If an arrow shot by an attacker traveled over the moat and outer wall, those inside the castle would be vulnerable to these attacks, even if there was a strong security perimeter. The solution is to provide each defender with a personal shield to deflect the arrows. This analogy also applies to information security. As important as a strong network security perimeter is to blocking attacks, some attacks will slip through the defenses. It is vital to also have local security on all of the personal computers to defend against any attack that breaches the perimeter.

Update Defenses

Imagine a castle in which each defender has been given a personal leather shield to protect him- or herself against arrows shot over the wall. The defenders may feel that they have adequate protection against the attacker's arrows. Yet what if suddenly the arrows came over the wall with their tips on fire? If the defenders have never seen flaming arrows before, they would be at a loss regarding how to prevent their leather shields from catching fire when struck with one of these arrows. This "new technology" of flaming arrows could prove to be disastrous if the defenders have no means to change their type of shields.

Today's information security attackers are equally, if not more, inventive than attackers of 1,000 years ago. New types of attacks appear daily. It is essential that users today continually update their defenses to protect their information. This involves updating defensive hardware and software as well as applying operating system security updates on a regular basis.

Minimize Losses

As a flaming arrow sails over the castle wall, it might strike a bale of hay and set it ablaze. If the defenders were not prepared with a bucket of water to douse the flames, then the entire castle could burn up. Being prepared to minimize losses was essential in defending a castle.

Likewise, in information security, it is important to realize that some attacks will get through security perimeters and local defenses. It is important that action be taken in advance in order to minimize losses. This may involve keeping backup copies of important data stored in a safe place, or, for an organization, it may mean having an entire business recovery policy that details what to do in the event of a successful attack.

Stay Alert

How protected would a castle be if the defenders were asleep or cowered in fear under a bed? It was vital that all those defending the castle would stay alert and be constantly vigilant to join the fight.

The same is true today. Information security cannot be considered the task of "somebody else" but is instead the responsibility of all users. This involves having the knowledge of what to do as well as the proper motivation to stay secure. And it requires constant vigilance as new attacks exploiting previously unknown vulnerabilities occur on a daily basis.

Chapter Summary

- Attacks against information security have grown exponentially in recent years, despite the fact that billions of dollars are spent annually on security. No computer system is immune to attacks or can be considered entirely secure.
- There are several reasons why it is difficult to defend against today's attacks. These include the fact that virtually all devices are connected to the Internet, the speed of the attacks, greater sophistication of attacks, the availability and simplicity of attack tools, faster detection of vulnerabilities by attackers, delays in security updating, weak security update distribution, distributed attacks coming from multiple sources, and user confusion.
- Information security can be defined as that which protects the integrity, confidentiality, and availability of information on the devices that store, process, and transmit information and is achieved through products, people, and policies and procedures. As with many advanced subjects, information security has its own terminology. A threat is an event or action that represents a danger to information assets, which is something that has value. A threat agent is a person or element that has the power to carry out a threat, usually by exploiting vulnerability, which is a flaw or weakness. A risk is the likelihood that a threat agent will exploit the vulnerability.
- The main goals of information security are to prevent data theft, thwart identity theft, avoid the legal consequences of not securing information, maintain productivity, and foil cyberterrorism.
- The types of people behind computer attacks fall into several categories. The term *cybercriminal* generally refers to someone who attacks computers, yet strictly speaking cybercriminals are a loose network of attackers, identity thieves, and financial

fraudsters who are more highly motivated, less risk averse, better funded, and more tenacious than an "ordinary" attacker. Script kiddies do their work by downloading automated attack software from websites and then using it to break into computers. A broker is an attacker who sells his knowledge of a vulnerability to others. One of the largest information security threats to a business actually comes from insiders who are employed there. Cyberterrorists are motivated by their principles and beliefs, and turn their attacks to the network and computer infrastructure to cause panic among citizens. Hactivists use attacks as a means of protest or to promote a political agenda. In recent years state-sponsored attackers have been funded by government agencies to attack foreign governments and even their own citizens whom they consider hostile or threatening.

- A practical, comprehensive security strategy involves four key elements. The first is to block attacks by having a strong security perimeter, both on the network and on the personal computer. Another strategy is to regularly update defenses to protect against the latest attacks. Also, it is important to minimize losses due to any attacks that may be successful. Finally, it is vital to constantly stay alert to attacks.

Key Terms

Definitions for key terms can be found in the Glossary for this text.

accounting
asset
authentication
authorization
availability
broker
confidentiality
cybercrime
cybercriminal
cyberterrorism
cyberterrorist
exploit kit
Gramm–Leach–Bliley Act (GLBA)
hactivist
Health Insurance Portability and Accountability Act (HIPAA)
identity theft
information security
insiders
integrity
Payment Card Industry Data Security Standard (PCI DSS)
risk
Sarbanes–Oxley Act (Sarbox)
script kiddie
state-sponsored attacker
threat
threat agent
threat likelihood
threat vector
vulnerability

Review Questions

1. Each of the following is a reason why it is difficult to defend against today's attackers except _____.
   a. faster detection of vulnerabilities
   b. complexity of attack tools
   c. user confusion
   d. greater sophistication of attacks

2. In a general sense "security" is _____.
   a. only available on specialized computers
   b. protection from only direct actions
   c. the steps necessary to protect a person or property from harm
   d. something that can be relatively easy to achieve
3. _____ ensures that only authorized parties can view the information.
   a. Integrity
   b. Confidentiality
   c. Availability
   d. Authorization
4. Why can brokers command such a high price for what they sell?
   a. Brokers are licensed professionals.
   b. The attack targets are always wealthy corporations.
   c. The vulnerability they uncover was previously unknown and is unlikely to be patched quickly.
   d. Brokers work in teams and all the members must be compensated.
5. Each of the following is a successive layer in which information security is achieved except _____.
   a. policies and procedures
   b. people
   c. products
   d. purposes
6. What is a person or element that has the power to carry out a threat?
   a. exploiter
   b. threat agent
   c. hazard element
   d. risk agent
7. In information security terminology a(n) _____ is a flaw or weakness that allows an attacker to bypass security protections.
   a. access
   b. vulnerability
   c. worm hole
   d. access control

8. _____ ensures that individuals are who they claim to be.
   a. Demonstration
   b. Authentication
   c. Accounting
   d. Certification
9. The _____ requires that enterprises must guard protected health information and implement policies and procedures to safeguard it.
   a. Hospital Protection and Insurance Association Agreement (HPIAA)
   b. Sarbanes–Oxley Act (Sarbox)
   c. Gramm–Leach–Bliley Act (GLBA)
   d. Health Insurance Portability and Accountability Act (HIPAA)
10. The motivation of _____ is attacking for the sake of their principles or beliefs.
   a. cyberterrorists
   b. insiders
   c. script kiddies
   d. computer spies
11. What is the difference between a hactivist and a cyberterrorist?
   a. A hactivist is motivated by ideology while a cyberterrorist is not.
   b. Cyberterrorists always work in groups while hactivists work alone.
   c. The aim of a hactivist is not to incite panic like cyberterrorists.
   d. Cyberterrorists are better funded than hactivists.
12. Keeping backup copies of important data stored in a safe place is an example of _____.
   a. minimizing losses
   b. sending secure information
   c. blocking attacks
   d. layering
13. Each of the following can be classified as an "insider" except _____.
   a. business partners
   b. contractors
   c. cybercriminals
   d. employees
14. What is an objective of state-sponsored attackers?
   a. to right a perceived wrong
   b. to spy on citizens
   c. to sell vulnerabilities to the highest bidder
   d. fortune over fame

15. Each of the following is a characteristic of cybercriminals except _____.
    a. low motivation
    b. better funded
    c. less risk averse
    d. more tenacious
16. Each of the following is a characteristic of cybercrime except _____.
    a. unauthorized attempts to access information
    b. targeted attacks against financial networks
    c. exclusive use of worms and viruses
    d. theft of personal information
17. An example of a(n) _____ is a software defect in an operating system that allows an unauthorized user to gain access to a computer without a password.
    a. asset exploit (AE)
    b. threat agent
    c. vulnerability
    d. threat
18. _____ requires banks and financial institutions to alert customers of their policies and practices in disclosing customer information and to protect all electronic devices and paper containing personally identifiable financial information.
    a. California Savings and Loan Security Act (CS&LSA)
    b. Sarbanes–Oxley Act (Sarbox)
    c. Gramm–Leach–Bliley Act (GLBA)
    d. USA Patriot Act
19. _____ ensures that the information is correct and no unauthorized person or malicious software has altered that data.
    a. Integrity
    b. Obscurity
    c. Layering
    d. Confidentiality
20. Protecting information is accomplished by_____.
    a. protecting the devices on which the information is found
    b. securing only local servers
    c. hiring an Information Security Officer (ISO)
    d. reducing risk factors

Hands-On Projects

Project 1-1: Examine Data Breaches—Textual

The Privacy Rights Clearinghouse (PRC) is a nonprofit organization whose goals are to raise consumers' awareness of how technology affects personal privacy and empower consumers to take action to control their personal information. The PRC maintains a searchable database of security breaches that impact consumer's privacy. In this project you will gather information from the PRC website.

1. Open a web browser and enter the URL **www.privacyrights.org/data-breach** (if you are no longer able to access the site through the web address, use a search engine to search for "Privacy Rights Clearinghouse data breach").
2. First spend time reading about the PRC. Click **About Us** in the toolbar.
3. Scroll down to the content under Mission and Goals and also under Services. Spend a few minutes reading about the PRC.
4. Click your browser's **Back** button to return to the previous page.
5. On the **Chronology of Data Breaches** page scroll down and observe the different breaches listed in chronological order.
6. Now create a customized list of the data that will only list data breaches of educational institutions. Scroll back to the top of the page.
7. Under **Select organization type(s)**, uncheck all organizations except **EDU - Educational Institutions**.
8. Click **GO!**.
9. Scroll down to **Breach Subtotal** if necessary. How many breaches that were made public pertain to educational institutions?
10. Scroll down and observe the breaches for educational institutions.
11. Scroll back to the top of the page. Click **New Search**, located beneath the **GO!** button.
12. Now search for breaches that were a result of lost, discarded, or stolen equipment that belonged to the government and military. Under **Choose the type of breaches to display**, uncheck all types except **Portable device (PORT) - Lost, discarded or stolen laptop, PDA, smartphone, portable memory device, CD, hard drive, data tape, etc.**
13. Under Select organization type(s), uncheck all organizations except **GOV – Government and Military**.
14. Click **GO!**.
15. Scroll down to Breach Subtotal, if necessary. How many breaches that were made public pertain to this type?
16. Scroll down and observe the breaches for governmental institutions.

17. Scroll back to the top of the page.
18. Now create a search based on criteria that you are interested in, such as the Payment Card Fraud against Retail/Merchants during the current year.
19. When finished, close all windows.

Project 1-2: Examine Data Breaches—Visual

In this project you will view the biggest data breaches resulting in stolen information through a visual format.

1. Open your web browser and enter the URL **http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/** (if you are no longer able to access the site through this web address, use a search engine to search for "Information Is Beautiful World's Biggest Data Breaches").
2. Click **Hide Filter** to display a visual graphic of the data breaches, as shown in Figure 1-6.

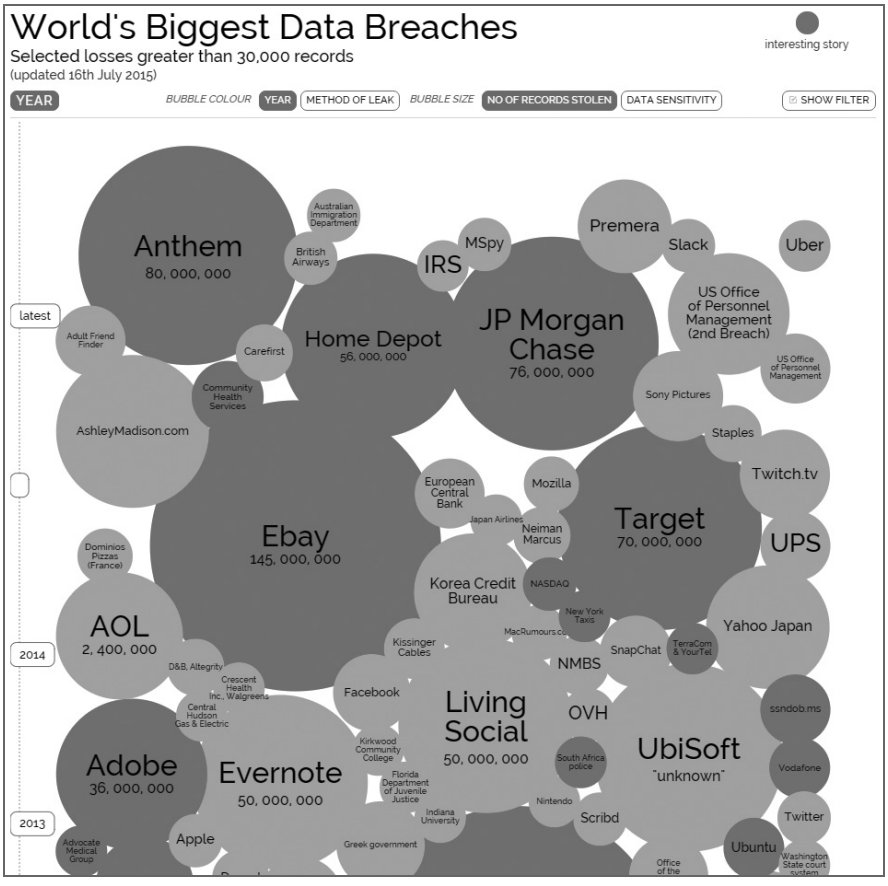


Figure 1-6 World's Biggest Data Breaches

Source: Information is Beautiful

3. Scroll down the page to view the data breaches. Note that the size of the breach is indicated by the size of the bubble.
4. Scroll back up to the top and note that the color of the bubbles that have an "Interesting Story." Click one of the bubbles and read the story.
5. Click **Read a bit more**.
6. Click **Click to see the original report**.
7. Read about the data breach. When finished close only this tab in your browser.
8. Click **Show Filter** to display the filter menu.
9. Under "Organisation" click **Retail**.
10. Under "Method of Leak" click **Hacked**. How many bubbles appear?
11. Under "Organisation" click **Government**.
12. Under "Method of Leak" click **Inside Job**. How many bubbles appear?
13. Under "Organisation" click **All**.
14. Under "Method of Leak" click **All**.
15. At the top of the graphic click **Method of Leak** so that the bubbles display how the leak occurred. Which type of leak is the most common? Why do you think this is the case?
16. Does this visual convey a better story than the textual data in the previous project?
17. Close all windows.

Project 1-3: Scan for Malware Using the Microsoft Safety Scanner

In this project you will download and run the Microsoft Safety Scanner to determine if there is any malware on the computer.

1. Determine which system type of Windows you are running. Click **Start**, **Control Panel**, **System and Security**, and then **System**. Look under **System type** for the description.
2. Open your web browser and enter the URL **www.microsoft.com/security/scanner/en-us/default.asp** (if you are no longer able to access the site through the URL, use a search engine to search for "Microsoft Safety Scanner").
3. Click **Download Now**.
4. Select either **32-bit** or **64-bit**, depending upon which system type of Windows you are running.
5. When the program finishes downloading, right-click **Start** and click **Open Windows Explorer**.
6. Click the **Downloads** icon in the left pane.

7. Double-click the **msert.exe** file.
8. Click **Run**. If the **User Account Control** dialog box appears, click **Yes**.
9. Click the check box to accept the license terms for this software. Click **Next**.
10. Click **Next**.
11. Select **Quick scan** if necessary.
12. Click **Next**.
13. Depending on your computer this scan may take several minutes. Analyze the results of the scan to determine if there is any malicious software found in your computer.
14. If you have problems you can click **View detailed results of the scan**. After reviewing the results, click **OK**. If you do not find any problems, click **Finish**.
15. If any malicious software was found on your computer run the scan again and select **Full scan**. After the scan is complete, click **Finish** to close the dialog box.
16. Close all windows.

Project 1-4: Write-Protecting a USB Flash Drive

Malicious software is often spread from one computer to another by infected USB flash drives. This can be controlled by write-protecting the drive so that no malware can be copied to it. In this project, you will download and install a software-based USB write blocker to prevent data from being written to a USB device. You will need a USB flash drive for this project.

1. Open your web browser and enter the URL **www.irongeek.com/i.php?page=security/thumbscrew-software-usb-write-blocker** (if you are no longer able to access the program through the URL, use a search engine to search for "Irongeek Thumbscrew").
2. Click **Download Thumbscrew**.
3. If the File Download dialog box appears, click **Save** and follow the instructions to save this file in a location such as your desktop or a folder designated by your instructor.
4. When the file finishes downloading, extract the files in a location such as your desktop or a folder designated by your instructor. Navigate to that location and double-click **thumbscrew.exe** and follow the default installation procedures.
5. After installation, notice that a new icon appears in the system tray in the lower right corner of the screen.
6. Insert a USB flash drive into the computer.
7. Navigate to a document on the computer.
8. Right-click the document and then select **Send to**.
9. Click the appropriate **Removable Disk** icon of the USB flash drive to copy the file to the flash drive.

10. Now make the USB flash drive write protected so it cannot be written to. Click the icon in the system tray.
11. Click **Make USB Read Only**. Notice that a red circle now appears over the icon to indicate that the flash drive is write protected.
12. Navigate to a document on the computer.
13. Right-click the document and then select **Send to**.
14. Click the appropriate **Removable Disk** icon of the USB flash drive to copy the file to the flash drive. What happens?
15. Click the icon in the system tray to change the permissions so that the USB drive is no longer read only.
16. Close all windows.

Case Projects

Case Project 1-1: Attack Experiences

Based on your personal experiences or those of someone you know (you may have to interview other students or a friend), write a paragraph regarding a computer attack that occurred. When did it happen? What was the attack? What type of damage did it inflict? Using the information in Table 1-2, list the reason or reasons you think that the attack was successful. How was the computer fixed after the attack? What could have prevented it? Write a one-page paper about these experiences.

Case Project 1-2: Information Security Community Site Activity

The Information Security Community website is an online companion to this textbook. It contains a wide variety of tools, information, discussion boards, and other features to assist learners. In order to gain the most benefit from the site, you will need to set up a free account. Go to **http://community.cengage.com/infosec2**. Click the "Join or Sign In" icon at the top of the page and then click **Join here**. On the Register page, enter the requested information (for your sign-in name use your first name and last name separated with a period or use the naming convention designated by your instructor). Explore the various features of the Information Security Community website, and become familiar with it. Visit the blog section and read the blog postings to learn about some of the latest events in IT security.

Additional Case Projects for this chapter are available through the MindTap online learning environment.

References

1. "2014 Year of Mega Breaches & Identity Theft." *Breach Level Index*. Accessed June 4, 2015. http://breachlevelindex.com/pdf/Breach-Level-Index-Annual-Report-2014.pdf.
2. "Top Health Industry Issues of 2015." *PriceWaterhouseCoopers*. Accessed June 4, 2015. http://www.pwc.com/en_US/us/health-industries/top-health-industry-issues/assets/pwc-hri-top-healthcare-issues-2015.pdf.
3. "Criminal Attacks: The New Leading Cause of Data Breach in Healthcare." *Ponemon Institute*. Accessed June 4, 2015. http://www.ponemon.org/blog/criminal-attacks-the-new-leading-cause-of-data-breach-in-healthcare.
4. "KCodes NetUSB: How a Small Taiwanese Software Company Can Impact the Security of Millions of Devices Worldwide." *SEC Consultant*. Accessed June 4, 2015. http://blog.sec-consult.com/2015/05/kcodes-netusb-how-small-taiwanese.html.
5. Greenberg, Andy, "Hackers Remotely Kill a Jeep on the Highway—with Me in It." *Wired*. July 21, 2015. Accessed Aug. 6, 2015. http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
6. "Recalls and Defects." *NHTSA*. Accessed Aug. 6, 2015. http://www.nhtsa.gov/Vehicle+Safety/Recalls+&+Defects.
7. Zetter, Kim, "Feds Say That Banned Researcher Commandeered a Plane." *Wired*. May 15, 2015. Accessed Aug 6, 2015. http://www.wired.com/2015/05/feds-say-banned-researcher-commandeered-plane/
8. Bilton, Nick, "Keeping Your Car Safe from Electronic Thieves." *The New York Times*. Apr. 15, 2015. Accessed Aug 6, 2015. http://www.nytimes.com/2015/04/16/style/keeping-your-car-safe-from-electronic-thieves.html?_r=0
9. "Damballa State of Infections Report Q4 2014." *Damballa*. Accessed June 4, 2015. https://www.damballa.com/state-infections-report-q4-2014/.
10. Lemos, Robert, "Madonna Turns to the Sneakernet after Album Leak." *Ars Technica*. Dec. 22, 2014. Accessed Aug 6, 2015. http://arstechnica.com/security/2014/12/madonna-turns-to-the-sneakernet-after-album-leak/.
11. "Hacking Tops List of Crimes Americans Worry about Most." Gallup. Accessed June 5, 2015. http://www.gallup.com/poll/178856/hacking-tops-list-crimes-americans-worry.aspx?utm_source=alert&utm_medium=email&utm_content=heading&utm_campaign=syndication.
12. "Mac Vulnerability Could Provide Persistent and Stealthy Access." *Symantec Security Response Blog*. Accessed June 5, 2015. http://www.symantec.com/connect/blogs/mac-vulnerability-could-provide-persistent-and-stealthy-access.
13. "Chronology of Data Breaches: Security Breaches 2005—Present." *Privacy Rights Clearinghouse*. Updated June 4, 2015. Accessed June 5, 2015. http://www.privacyrights.org/data-breach.
14. *Privacy Rights Clearinghouse*. Accessed June 5, 2015. https://www.privacyrights.org/data-breach.

15. "Malware." AVTest. May 28, 2015. Accessed June 5, 2015. www.av-test.org/en/statistics/malware/.

16. "Someone Filed a False Tax Return in Your Name. What Now?" *U.S. News Money*. Accessed June 9, 2015. http://money.usnews.com/money/personal-finance/articles/2015/03/17/someone-filed-a-false-tax-return-in-your-name-what-now.

17. "Ripping off Uncle Sam," *Bloomberg BusinessWeek*. Apr. 13, 2015. Accessed June 9, 2015, http://www.ritholtz.com/blog/2015/04/ripping-off-uncle-sam/.

18. Reed, John, "Cyber Terrorism Now at the Top of the List of Security Concerns." *Defensetech*. Accessed Jan. 27, 2013. http://defensetech.org/2011/09/12/cyber-terrorism-now-at-the-top-of-the-list-of-security-concerns/.

19. Goldman, David, "Hacker Hits on U.S. Power and Nuclear Targets Spiked in 2012." *CNN Money*. Jan. 9, 2013. Accessed Jan. 27, 2014. http://money.cnn.com/2013/01/09/technology/security/infrastructure-cyberattacks/.

20. Sweeney, Patrick, "Defending against Exploit Kits," *Network World*. June 3, 2013. Accessed Dec. 7, 2013. www.networkworld.com/news/tech/2013/060313-exploit-kits-270404.html.

21. "Google Paid over $1.5 Million in Bug Bounties in 2014." *InformationWeek Dark Reading*. Jan. 30, 2015. Accessed June 10, 2015. http://www.darkreading.com/vulnerabilities—threats/google-paid-over-$15-million-in-bug-bounties-in-2014/d/d-id/1318886.

22. "2014 Highlights: Bounties Get Better than Ever." *Facebook*. Feb. 25, 2015. Accessed June 10, 2015. https://www.facebook.com/notes/facebook-bug-bounty/2014-highlights-bounties-get-better-than-ever/1026610350686524.

23. Cappelli, Dawn, "Internal Review: The Insider Threat Risk." *SC Magazine*. Feb. 2, 2011. Accessed Feb. 28, 2011. http://inform.com/government-and-politics/internal-review-insider-threat-risk-4737197a.

24. ibid.

chapter 2

Personal Security

After completing this chapter you should be able to do the following:

- Define what makes a weak password
- Describe the attacks against passwords
- Identify the different types of social engineering attacks
- Describe identity theft and the risks of using social networking
- Describe personal security defenses

Security in Your World

"Who cares?" laughed Santiago. Moritz looked up from his book and asked, "What's going on?" Santiago and Moritz were studying at the school's library before their next class. "I just got an email that says, 'Your Zebra File Storage account may have been compromised. Zebra has discovered evidence that user passwords were stolen by unknown attackers. Click this link to reset your password.' I don't care if they have my password," said Santiago as he set down his smartphone. "Why not?" asked Moritz. "Oh, I never use that account very much. I don't even remember what I have stored there," Santiago answered.

"I know what you mean," said Moritz. "If I started changing my password for one account then I'll never remember it. I just use the same password everywhere." Santiago leaned back in his chair. "Doesn't everybody? How could you remember all of your passwords if you had different ones?"

"Excuse me." Santiago and Moritz looked up. "I couldn't help but overhear your conversation about passwords. I'm Anastasiya, and I work at the Student Help Desk answering phone calls. If you've ever called the Help Desk you may have talked with me."

"That's OK," said Moritz. "We probably shouldn't even be talking this loud in the library. They may run us out!"

Anastasiya laughed. "I know. Anyway, all the student workers at the Help Desk had a meeting earlier this week with the school's Director of Security about passwords and he told us some stuff that I hadn't thought of about passwords." "Like what?" asked Santiago. "He said that attackers have stolen hundreds of millions of passwords and they now use all of those to break into user's accounts. Because most people use the same password for most or all of their accounts, a password that was stolen from one account can be used to get into other accounts. It's like having a master key to all of the doors of an office building," Anastasiya said. Santiago and Moritz looked at each other. They both used the same password on all of their accounts.

"And that's not all," Anastasiya continued. "He said that people who do use different passwords will divide their accounts into those that they think need a strong password and those that don't. But they forget that an account that seems like it doesn't need a strong password really should have one." "Why?" asked Moritz. "He said that email accounts usually are given weak passwords because we don't think they are important," Anastasiya said. "But actually they are very important. When you have to reset a password that you forgot, an email with a password reset link is sent to your email account." Moritz said, "I'm not sure I understand."

Anastasiya set down her backpack and said, "Well, suppose an attacker stole your Gmail password. She could go to your Zebra File Storage account and just

click 'Forgot my password.' That password reset link would be mailed to your Gmail account. Because the attacker stole your Gmail password she could then get into your Gmail account, open the email from Zebra and click the password reset link, and then reset your Zebra password to whatever she wanted to. And then she could log in your Zebra account and change the email address for the password reset link so that it now goes to her own email account. That way you could never log in to your Zebra account or even reset your own password even if you wanted to."

"Wow!" said Santiago. "I never thought of that. What else did he say?"

Many early computer attacks were malicious in nature: they were intended to erase a user's data on the computer or corrupt the hard disk drive so that the computer could not properly function. These types of attacks are similar to vandalism, where the goal is to deface or destroy.

Today, however, most attacks are not designed to *destroy* data on the computer; instead, these attacks attempt to *steal* that data and then use it for financial gain. For example, some attacks trick users into revealing personal information such as a credit card number or password in response to a fictitious email that pretends to come from a reputable bank. Other attacks take advantage of the fact that many users reuse the same password on multiple accounts or create short passwords that are relatively easy to break. And some attacks take advantage of the trusting relationships that often exist in social-networking sites: an attacker pretends to be an "old high school friend" and convinces the victim to open a file that secretly installs malicious software that monitors keystrokes, in order to steal passwords or bank card numbers.

These types of attacks are directly aimed at the user's personal security and are not always strictly targeted at specific types of devices or certain kinds of software. Rather, these attacks impact users of desktop computers, smartphones, tablets, and laptops using Microsoft Windows, Apple Mac OS and iOS, Android, or other operating systems. Because these attacks are aimed at the user's personal security, no matter what type of device they may be using, the defenses against these attacks can apply broadly to all devices and all users.

This chapter examines attacks directed at users and their personal security. First, you'll explore personal security attacks that target passwords and also that take advantage of social engineering. Then, you'll look at identity theft and risks associated with using social networking. Finally, you will learn about the defenses you can use to protect yourself from attacks on your personal security.

Personal Security Attacks

There are different attacks that are launched against a user's personal security. These attacks include password attacks, attacks using social engineering, identity theft, and social networking attacks.

Password Attacks

In most instances, a user logging in to a computer or a website would be asked to *identify* himself. This is done by entering an identifier known as the **username**, such as *SListz*. Yet because anyone could enter this username, the next step is for the user to *authenticate* himself by proving that he actually is *SListz*. Providing proof of his genuineness (a process known as **authentication**) confirms his identity and can be used to protect the user's important assets by preventing access by an imposter.

The most common means of authentication is by providing information that only the genuine user knows: because only the real or "authentic" *SListz* uniquely knows this information it can be used to confirm his identity. The information that is uniquely known is called a password. A **password** is a secret combination of letters, numbers, and/or characters that—ideally—only the user would know.

What an individual uniquely knows—a password—is not the only type of authentication that can be used. In addition to what the user knows, other types of authentication are where she is, what she has, what she is, and what she does.

Passwords are the most common type of authentication used today. However, despite their widespread use, most passwords provide only weak protection. These weaknesses open the door for attacks on passwords.

Password security has been exploited since the early days of computers. In 1961 MIT developed the Compatible Time-Sharing System (CTSS) in which passwords were first used to authenticate computer users. In the spring of 1962, a Ph.D. researcher who had been allotted only four hours per week of computing resources submitted a request to the CTSS computer to print the list of all password files. Because there were no safeguards, the computer produced the list, which the researcher then used to log in with other users' passwords to gain more computing time.

Password Weaknesses The strength of passwords—that they are based on human memory—is also the weakness of passwords. That is because human beings can memorize only a limited number of items. Passwords place heavy loads on memory in multiple ways:

- The most effective passwords are long and complex. However, these are difficult for users to memorize and then accurately recall when needed. And each password used should be unique, which further strains human memory.
- Users must remember passwords for many different accounts. These include computers and mobile devices used at work, school, and home; multiple web accounts; online banking; email accounts; social media accounts; and so on. In one study, 28 percent of a group of users had more than 13 passwords each,[1] while in another study a group of 144 users had an average of 16 passwords per user.[2] And users aged 16–24 had an average of 6.6 different accounts just for social media sites like Facebook, Twitter, and Instagram.[3]

- Many business systems have strict security policies that mandate passwords expire after a set period of time, such as every 45–60 days, when a new one must be created. Some security policies even prevent a previously used password from being recycled and used again, forcing users to repeatedly memorize new passwords.

Because of the burdens that passwords place on human memory, users take shortcuts to help them memorize and recall their passwords. These shortcuts produce a **weak password**, or one that is easy for an attacker to break. Weak passwords often use a common word as a password (*princess*), a short password (*desk*), a predictable sequence of characters (*abc123*), or personal information (*Hannah*) in a password. Another common shortcut is to reuse the same password for multiple accounts. Although this makes it easier for the user, it also makes it easier for an attacker who compromises one account to access the user's other accounts.

Even when users attempt to create stronger passwords, they generally follow predictable patterns of appending (adding a number or mark of punctuation only to the end of a password) or replacing, such as substituting a zero for the letter *o* (*passw0rd*), the digit *1* for the letter *i* (*denn1s*), or a dollar sign for an *s* (*be$tfriend*). Attackers are aware of these patterns and can search for them in passwords, making it easier to break them.

The alarming use of weak passwords can be easily illustrated. Several recent attacks have resulted in hundreds of millions of user passwords being stolen, many of which were then posted on the Internet. An analysis of one theft of 32 million user passwords showed that 30 percent of users had created passwords of only five or six characters, while just 12 percent of the user passwords were nine characters in length, which is still considered too short to be effective. Almost one in every five users created a password that was one of the 5,000 most common passwords, including names, slang words, dictionary words, or trivial passwords (consecutive digits, adjacent keyboard keys, etc.). The 10 most common passwords found and their number of occurrences are listed in Table 2-1.

Rank	Password	Number of users with password
1	123456	290,731
2	12345	79,078
3	123456789	76,790
4	Password	61,958
5	iloveyou	51,622
6	princess	35,231
7	rockyou	22,588
8	1234567	21,726
9	12345678	20,553
10	abc123	17,542

Table 2-1 Ten most common passwords

Unfortunately some websites make it difficult for users to have strong passwords. Sometimes the maximum number of characters allowed for a password is restricted to a length that is too short to provide strong security. Other websites will only accept letters or numbers as part of a password and prohibit the use of characters (@, #, or $) that would make the password stronger. And some websites prevent the user from pasting a long password into the website's login prompt, thus forcing the user to rely strictly on memory.

A noted security expert summarized the password problem well by stating:

> *The problem is that the average user can't and won't even try to remember complex enough passwords to prevent attacks. As bad as passwords are, users will go out of the way to make it worse. If you ask them to choose a password, they'll choose a lousy one. If you force them to choose a good one, they'll write it [down] and change it back to the password they changed it from the last month. And they'll choose the same password for multiple applications.*[4]

Attacks on Passwords There are a variety of attacks that can be used to uncover a password. One attack technique that is *not* used is *online guessing* in which the attacker attempts to randomly guess the password by typing different variations at the password login prompt. Most accounts are set to disable all logins after a limited number of incorrect attempts (such as five), thus locking out the attacker. And even if the attacker had an unlimited number of attempts it would still take an unreasonable amount of time to attempt all of the different combinations in order to guess the right password.

An attacker trying to break a short eight-character password that is made up from 76 characters (uppercase and lowercase letters, digits, and common symbols) entering two or three passwords per second may have to spend up to *5,878,324 years* to guess the right password.

Because of the limitations of online guessing, most password attacks today use *offline cracking*. When a password is first created by the user, usually a digital representation of that password is created and stored on the computer or website (technically speaking, the process for creating this digital representation is based on a *hash algorithm,* which creates a *digest*). For example, the digest for the password *jurghbtref* could be calculated as *38e6b7cb3b7e66777c625fade02736e9* and is then stored on the computer or website. When a user later reenters her password to log on, the same hash algorithm is applied to what she just typed into the password login prompt and then compared with the stored version; if it matches, the user is approved. This is illustrated in Figure 2-1.

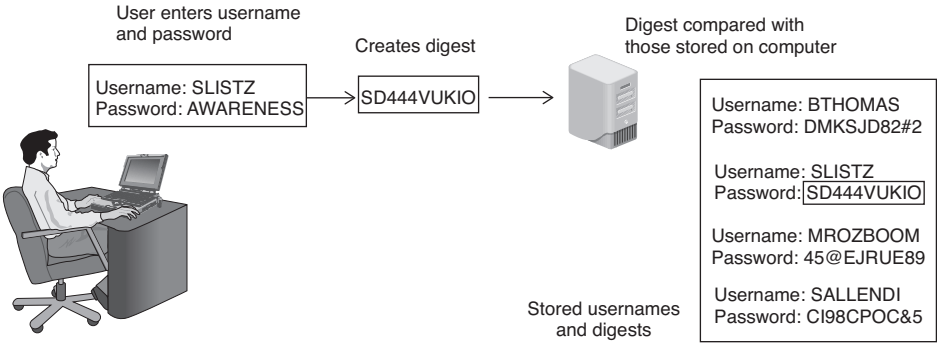


Figure 2-1 Comparing password digests

With offline cracking, attackers steal the file of password digests and then use their own powerful computers to break the passwords. The attackers do this by first creating their own passwords and then generating the digests (called *candidates*) for these passwords. They then compare their digests against the stolen digests: when the digests match then the attackers will know the password behind the digest.

The advantage of offline cracking is that it allows the attacker to use fast technology to break a password instead of manual random guesses. One security researcher created a computer cluster of five server computers and was able to generate 350 billion password candidates per second.[5]

Several offline cracking techniques attempt to match a known candidate password digest with stolen digests. In an automated **brute force attack**, every possible combination of letters, numbers, and characters is used to create candidate digests that are then matched against those in the stolen digest file. This is the slowest yet most thorough method. Using an automated brute force attack program, an attacker enters into the attack program such parameters as *password length* (the minimum and maximum lengths of the passwords to be generated such as a range from *1 to 45*), *character set* (the set of letters, symbols, and characters that make up the password), *language* (such as Arabic, Dutch, English, French, German, Italian, Portuguese, Russian, or Spanish), *mask* (if any part of the password is known, a pattern can be entered to reduce the number of passwords generated so that if the first two letters of a six-character password were known to be *sk*, the pattern could be *sk????*), and *skips* (because most passwords are wordlike combinations of letters the programs can be set to skip nonsensical combinations of characters (*wqrghea*) so that only passwords such as *elmosworld* and *carkeys* are created).

Another common password attack is a **dictionary attack**. A dictionary attack begins with the attacker creating digests of common dictionary words as candidates and then comparing them against those in a stolen digest file. A dictionary attack is shown in Figure 2-2.

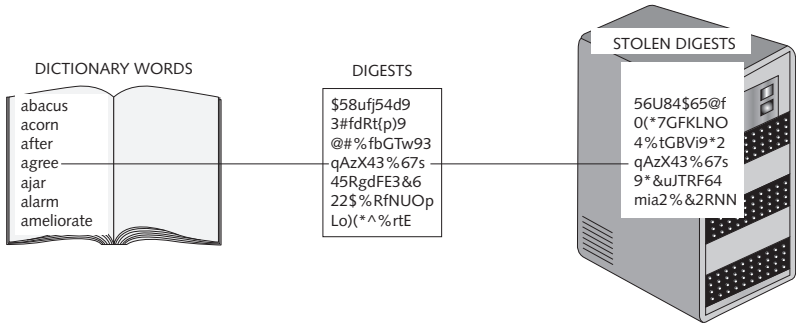


Figure 2-2 Dictionary attack

Dictionary attacks can be successful because users most often create passwords that are simple dictionary words.

However, a watershed moment in password attacks occurred in late 2009. An attacker broke into a server belonging to a developer of several popular social media applications. This server contained more than 32 million user passwords, all in cleartext (not as digests). These passwords were later posted on the Internet.

Attackers seized this opportunity to examine actual user passwords. These passwords provided two key elements for password attacks. First, this "treasure-trove" collection of passwords gave attackers, for the first time, a large corpus of real-world passwords. Because users repeat their passwords on multiple accounts, attackers could now use these passwords as candidate passwords in their attacks. It is estimated that in excess of hundreds of millions of passwords were stolen and published online in one year alone. Websites now host lists of these leaked passwords along with statistical analysis that attackers can utilize.

In addition, these password collections have given attackers insight into the strategic thinking of how users create passwords. For example, on those occasions when users mix uppercase and lowercase in passwords, users tend to capitalize at the beginning of the password, much like writing a sentence. Likewise, punctuation and numbers are more likely to appear at the end of the password, again mimicking standard sentence writing. And a high percentage of passwords were comprised of a name and date, such as *Braden2008*. Such insights can be valuable to attackers in designing a mask (such as *?dabcdef -2 ?l?u ?1?1?2?2?2?2?2*) to crack passwords, since using masks can significantly reduce the amount of time needed to break a password.

Attacks Using Social Engineering

Consider the following situations:

- *Unexpected email*. An unanticipated email arrives from a friend that contains a link to a website with the instructions "You've just got to check this out!" or has a file attachment with the message, "Is this really a picture of you?!?"

- *Urgent plea for help*. An email from an acquaintance says that she was traveling overseas but was robbed and beaten. She's now recovering but is in desperate need of money, and she asks that you wire money to the following account immediately.
- *Text message warning*. You receive a text message on your phone that says it is from your bank and you should call the following number immediately. Upon calling you hear an automated message that says, *"A text message has been sent to inform you that your debit card has been limited due to a security issue. To reactivate, please press 1 now."* After pressing 1 you are then prompted to enter last four digits of your Social Security number, and then full card number and expiration date of your debit card.
- *Disaster video*. Following a recent flood you search the Internet for information about how to donate to the victims. One professional-looking website contains a video with information about the disaster and how you can help and informs you to download a video and play it on your computer.

Each of these actual situations are using trickery to convince the victim to quickly perform a risky action that may in turn lead to a successful attack, as shown in Table 2-2. This is known as **social engineering**, or a means of manipulating users to perform an action or gather confidential information that can then be used by the attacker. Unlike most types of attacks, social engineering does not rely directly on technology, but instead relies on the actions of the victims.

Situation	Action asked to perform	Potential result
Unexpected email	Click on link or open attachment	Computer may become infected with malware
Urgent plea for help	Send money to account	Money sent to attacker's account
Text message warning	Provide bank card information	Attacker now has card information
Disaster video	Download video to computer	Downloaded video may contain malware

Table 2-2 Social engineering attacks

Social media sites such as Facebook are popular with attackers to create a trust relationship with a user and then gather information.

At its core, social engineering relies on an attacker's clever manipulation of human nature in order to persuade the victim to provide information or take actions. Several basic "principles" or reasons make this type of social engineering effective. These are listed in Table 2-3 with the example of an attacker pretending to be the chief executive officer (CEO) calling the organization's help desk to have a password reset.

Principle	Description	Example
Authority	Directed by someone impersonating authority figure or falsely citing their authority	"I'm the CEO calling."
Intimidation	To frighten and coerce by threat	"If you don't reset my password, I will call your supervisor."
Consensus/social proof	Influenced by what others do	"I called last week and your colleague reset my password."
Scarcity	Something is in short supply	"I can't waste time here."
Urgency	Immediate action is needed	"My meeting with the board starts in 5 minutes."
Familiarity/liking	Victim is well known and well received	"I remember reading a good evaluation on you."
Trust	Confidence	"You know who I am."

Table 2-3 Social engineering effectiveness

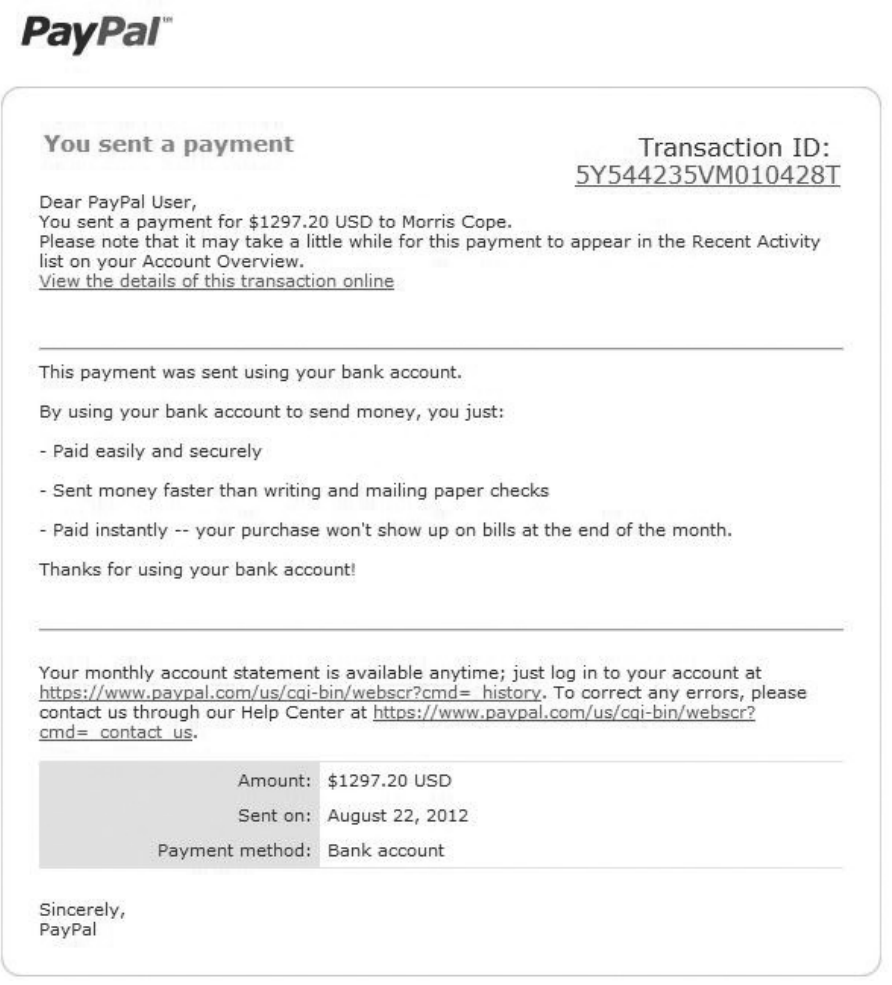
Because some of the approaches involve person-to-person contact directly or over the phone, attackers use a variety of techniques to gain trust without moving quickly so as to become suspicious. Often attackers will use flattery, flirtation, or a simple "I'm confused, can you please help me?" to "soften up" the victim to cooperate.

Social engineering attacks involve phishing, typo squatting, pretexting, hoaxes, dumpster diving, and shoulder surfing.

Phishing One of the most common forms of social engineering is phishing. **Phishing** is sending an email or displaying a web announcement that falsely claims to be from a legitimate enterprise in an attempt to trick the user into surrendering private information. Users are asked to respond to an email or are directed to a website where they are requested to update personal information, such as passwords, credit card numbers, Social Security numbers, bank account numbers, or other information. However, the email or website is actually an imposter site that is set up to steal what information the user enters.

The word *phishing* is a variation on the word "fishing," with the idea being that bait is thrown out knowing that while most will ignore it, some will "bite."

One of the reasons that phishing succeeds is that the emails and the fake websites appear to be legitimate. Figure 2-3 illustrates an actual phishing email message that claims the victim has recently made a large payment to an individual. The message contains the logos, color schemes, and wording used by the legitimate site so that it appears to be genuine. The victim would naturally be puzzled by this message and click the links, which would then ask for a username and password to log in, but instead of accessing a legitimate site, this information is captured by the attacker.



PayPal™

You sent a payment

Transaction ID:
5Y544235VM010428T

Dear PayPal User,
You sent a payment for $1297.20 USD to Morris Cope.
Please note that it may take a little while for this payment to appear in the Recent Activity list on your Account Overview.
View the details of this transaction online

This payment was sent using your bank account.

By using your bank account to send money, you just:

- Paid easily and securely

- Sent money faster than writing and mailing paper checks

- Paid instantly -- your purchase won't show up on bills at the end of the month.

Thanks for using your bank account!

Your monthly account statement is available anytime; just log in to your account at https://www.paypal.com/us/cgi-bin/webscr?cmd=_history. To correct any errors, please contact us through our Help Center at https://www.paypal.com/us/cgi-bin/webscr?cmd=_contact_us.

Amount:	$1297.20 USD
Sent on:	August 22, 2012
Payment method:	Bank account

Sincerely,
PayPal

Figure 2-3 Phishing email message

Source: PayPal

Several variations on phishing attacks are:

- *Spear phishing*. Whereas phishing involves sending millions of generic email messages to users, **spear phishing** targets only specific users. The emails used in spear phishing are customized to the recipients, including their names and personal information, in order to make the message appear legitimate.
- *Whaling*. One type of spear phishing is **whaling**. Instead of going after the "smaller fish," whaling targets the "big fish," namely, wealthy individuals or senior executives within a business who typically would have larger sums of money in a bank account that an attacker could access if the attack is successful. By focusing upon this smaller group, the attacker can invest more time in the attack and finely tune the message to achieve the highest likelihood of success.

- *Vishing*. Instead of using email to contact the potential victim, a telephone call can be used instead. Known as **vishing** (*voice phishing*), an attacker calls a victim who, upon answering, hears a recorded message that pretends to be from the user's bank stating that her credit card has experienced fraudulent activity or that her bank account has had unusual activity. The victim is instructed to call a specific phone number immediately (which has been set up by the attacker). When the victim calls, it is answered by automated instructions telling her to enter her credit card number, bank account number, Social Security number, or other information on the telephone's key pad.

Typo Squatting What happens when a user makes a typing error when entering a uniform resource locator (URL) address in a web browser, such as typing *goggle.com* (a misspelling) or *google.net* (incorrect domain) instead of the correct *google.com*? Most often, the user will be directed to a fake look-alike site. This site may contain a visitor survey that promises a chance to win prizes (but the attacker actually captures the entered email addresses to sell to spammers) or be filled with ads (for which the attacker receives money for traffic generated to the site). These fake sites exist because attackers purchase the domain names of sites that are spelled similarly to actual sites. This is called **typo squatting** (also called *URL hijacking*). A well-known site like *google.com* may have to deal with more than 1,000 typo squatting domains. Over 62 percent of the active domain names based on common misspellings of *facebook.com* are typo squatting sites.

The cost of typo squatting is significant because of the large number of misspellings. In one month the typo squatting site *goggle.com* received almost 825,000 unique visitors. It is estimated that typo squatting costs the 250 top websites $285 million annually in lost sales and other expenses.[6]

While a typing error when entering a URL to visit a webpage can be a problem, an even larger problem is the fact that attackers also receive all private email messages that had similar typing errors (such as an email sent to *finances@goggle.com*). Security researchers set up fake domains based on the names of the 500 largest U.S. companies that only omitted the period between the domain name and subdomain. In six months they received more than 120,000 private emails (or 20 gigabytes worth of email) based on this one typing error, many containing confidential information and even lists of passwords.[7]

Pretexting Social engineering **pretexting** is creating an invented scenario (the *pretext*) to persuade the victim to perform an action or provide confidential information. While it involves lying, pretexting is considered to be much more than just creating a lie; it can fabricate an entirely new identity to use in the attack.

Pretexters use different tactics to acquire information. In one example a pretexter might call a person and claim to be from a firm that conducts surveys to ask what seems to be a series of harmless questions. After finishing that call the pretexter then calls a company with whom that person conducts business. The pretexter then claims to be that person and pretends that he has forgotten his account number or needs information about his account history. Through this social engineering attack the pretexter may be able to obtain personal information about the victim such as Social Security Number, bank and credit card account numbers, credit report information, and the size of savings and investment portfolios.

Some information is considered public record, such as owning a home, paying real estate taxes, or filing for bankruptcy, and can easily be collected through an online search. However, it is illegal for someone to use false, fictitious or fraudulent statements or documents to receive customer information from a financial institution or directly from a customer of a financial institution.

Hoaxes Attackers can use hoaxes as a first step in an attack. A **hoax** is a false warning, often contained in an email message claiming to come from the information technology (IT) department. The hoax purports that there is a "deadly virus" circulating through the Internet and that the recipient should erase specific files or change security configurations, and then forward the message to other users. However, changing configurations allows an attacker to compromise the system. Or, erasing files may make the computer unstable, prompting the victim to call the telephone number in the hoax email message for help, which is actually the phone number of the attacker.

Dumpster Diving **Dumpster diving** involves digging through trash receptacles to find information that can be useful in an attack. Table 2-4 lists the different items that can be retrieved from a business—many of which appear to be useless—and how they can be used.

Item retrieved	Why useful
Calendars	A calendar can reveal which employees are out of town at a particular time.
Inexpensive computer hardware, such as USB flash drives or portal hard drives	These devices are often improperly disposed of and may contain valuable information.
Memos	Seemingly unimportant memos can often provide small bits of useful information for an attacker who is building an impersonation.
Organizational charts	These identify individuals within the organization who are in positions of authority.
Phone directories	A phone directory can provide the names and telephone numbers of individuals in the organization to target or impersonate.
Policy manuals	These may reveal the true level of security within the organization.
System manuals	A system manual can tell an attacker the type of computer system that is being used so that other research can be conducted to pinpoint vulnerabilities.

Table 2-4 Dumpster diving items and their usefulness

Dumpster diving is not confined to businesses. Often attackers will look through the trash receptacles of homeowners to steal preapproved credit card offers, documents containing Social Security numbers, email addresses, bank account information, and employment history all of which can be used in attacks.

Shoulder Surfing Consider this scenario: A man walks up to a bank's automated teller machine (ATM) located on a busy downtown street to make a deposit. After inserting his ATM card the machine asks him to enter his personal identification number (PIN) on the

keypad. As he types in the four-digit number, he notices that a young woman has walked up behind him and is waiting to use the ATM. As the man navigates through the menus, the woman begins to mutter, "Come on, come on, come on. I've got to get going!" Flustered by the woman's impatience the man clicks on an incorrect menu option and then has to backtrack through several additional options. The woman sighs loudly and then says, "Are you almost finished?" The man hurriedly completes his deposit, takes his receipt and card, and quickly walks away. That evening, when he returns home, he checks his online bank account and discovers that five cash withdrawals from his account occurred at the same ATM for $200, $100, $200, $100, and $200 all within one minute of his original transaction.

This man was the victim of **shoulder surfing**, in which information entered is observed by another person. In this incident after the man completed his transaction on the ATM the message "Do you want to perform another transaction?" appeared on the screen. Because he already had his card and receipt the man just walked away. However, the question remained on the screen long enough for the woman behind him to tap the "YES" key and reenter his PIN, which she had watched him enter. This gave her the opportunity to make the withdrawals from his account.

Shoulder surfing can be performed in virtually any public location where an individual is asked to enter personal identification. This includes entering a PIN at an ATM, completing a purchase in a store by entering a debit card PIN at the register, writing down a Social Security number on a paper form, or entering a password on a computer keyboard in a coffee shop or airport. Casually observing what is entered can be done from a distance of up to 15 feet (4.5 meters). More sophisticated techniques include using binoculars (such as in a large train or airport terminal) or using small closed-circuit television cameras that are concealed in a book or backpack.

Identity Theft

Identity theft involves using someone's personal information, such as their name, Social Security number, or credit card number, to commit financial fraud. Using this information to obtain a credit card, set up a cellular telephone account, or even rent an apartment, thieves can make excessive charges in the victim's name. The victim is charged for the purchases and suffers a damaged credit history that can be the cause for being turned down for a new job or denied loans for school, cars, and homes.

The following are some of the actions that can be undertaken by identity thieves:

- Produce counterfeit checks or debit cards and then remove all money from the bank account
- Establish phone or wireless service in the victim's name
- File for bankruptcy under the person's name to avoid eviction
- Go on spending sprees using fraudulently obtained credit and debit card account numbers to buy expensive items such as large-screen televisions that can easily be resold
- Open a bank account in the person's name and write bad checks on that account
- Open a new credit card account, using the name, date of birth, and Social Security number of the identity-theft victim. When the thief does not pay the bills, the delinquent account is reported on the victim's credit report.
- Obtain loans for expensive items such as cars and motorcycles

Table 2-5 summarizes some of the ways in which attackers can steal personal information.

Technique	Explanation
Dumpster diving	Discarded credit card statements, charge receipts, and bank statements can be retrieved for personal information.
Phishing	Attackers convince victims to enter their personal information at an imposter website after receiving a fictitious email from a bank.
Change of address form	Using a standard change-of-address form the attackers divert all mail to their post office box so that the victim never sees any charges made.
Pretexting	An attacker who pretends to be from a legitimate research firm asks for personal information.
Stealing	Stolen wallets and purses contain personal information that can be used in identity theft.

Table 2-5 How attackers steal personal information

One of the areas of identity theft that is growing most rapidly involves identity thieves filing fictitious income tax returns with the U.S. Internal Revenue Service (IRS). Identity thieves who steal a filer's Social Security number will then file a fake income tax return claiming a large refund—often larger than the victim is entitled to—that is sent to the attacker. Because the IRS has been sending refunds more quickly than in the past it has made it easier for thieves to receive the refund and then disappear before the victim files a legitimate return and the fraud is then detected. According to the IRS, it delivered over $5.8 billion in refund checks to identity thieves who filed fraudulent tax returns for 2013, even though it stopped about 3 million fraudulent returns for that year.[8]

Identity thieves are also known to set up fake tax preparation service centers to steal tax information from victims. One group filed $3.4 million worth of fraudulent returns through a sham tax preparation business.[9]

Social-Networking Risks

Grouping individuals and organizations into clusters based on their likes and interests is called **social networking**. The popularity of online social networking has skyrocketed. Social-networking websites facilitate linking individuals with common interests and function as an online community of users. A user on a social-networking site can read information posted by others and share documents, photos, and videos.

In the fall of 2008 Facebook reached 100 million users. By 2012 it had surpassed one billion users. Just three years later the number of users had increased by almost 50 percent to 1.49 billion monthly active users.[10]

Although using any website has risks associated with it, social-networking sites can carry additional risks. These risks include:

- *Personal data can be used maliciously*. Users post personal information on their pages for others to read, such as birthdays, where they live, their plans for the

upcoming weekend, and the like. However, attackers can use this information for a variety of malicious purposes. For example, knowing that a person is on vacation could allow a burglar to break into an empty home, the name of a pet could be a weak password that a user has created, or too much personal information could result in identity theft.

- *Users may be too trusting*. Attackers often join a social-networking site and pretend to be part of the network of users. After several days or weeks, users begin to feel they know the attackers and may start to provide personal information or click on embedded links provided by the attacker that loads malware onto the user's computer.
- *Social-networking security is lax or confusing*. Because social-networking sites by design are intended to share information, these sites have often made it too easy for unauthorized users to view other people's information. To combat this many sites change their security options on a haphazard basis, making it difficult for users to keep up with the changes.
- *Accepting friends may have unforeseen consequences*. Some social-networking users readily accept any "friend" request they receive, even if they are not familiar with that person. This can result in problems, since whomever is accepted as a friend may then be able to see not only all of that user's personal information but also the personal information of their friends.

Security in Your World

After listening to Anastasiya's information about passwords, Santiago reached over to Moritz's laptop computer on the table. "OK, you convinced me," he said. "I'm going to click on that Zebra password reset link and change my password right now." After a moment Moritz said, "Hey, wait a minute. How do you know that email is really from Zebra? What if it's one of those fake emails from the bad guys? Should he do that, Anastasiya?"

Anastasiya shook her head and said, "Moritz is right. That could be a phishing email trying to get you to enter your Zebra username and password so the attackers would then grab it. I don't think I'd do that if I were you."

Moritz took his hand off the mouse and said, "So what should I do?" Anastasiya opened her backpack and said, "Why don't you first think about your passwords." Moritz laughed and said, "That shouldn't take very long, since he only has one password that he uses everywhere!" Anastasiya smiled. "Not a good thing to do. Here, let me show you this program our Director of Security showed us. This is using technology instead of our memory for storing passwords." Santiago leaned forward and said, "Show it to me."

Personal Security Defenses

Despite the growing number of attacks on users' personal security, there are defenses that can be used to ward off these attacks. These defenses include using strong passwords, recognizing phishing attacks, taking steps to avoid identity theft, and securing social-networking sites.

Password Defenses

The best approach to establishing strong security with passwords is to use technology for managing passwords. If these tools are not used then techniques for creating and memorizing strong passwords must instead be implemented.

Using Password Management Tools In addition to the characteristics listed previously regarding weak passwords (such as using a common dictionary word, creating a short password, or using personal information in a password), there are two additional characteristics of weak passwords:

- Any password that can be *memorized* is a weak password.
- Any password that is *repeated* on multiple accounts is a weak password.

Because of the limitations of human memory and the fast processing speed of today's computers used by attackers, it is not possible for the average user to memorize multiple long passwords that can resist attacks. Instead of relying on human memory for passwords, security experts today recommend that technology be used instead to store and manage passwords. Technologies used for securing passwords are called **password managers**. There are three basic types of password managers:

- *Password generators.* These are web browser extensions that generate passwords. The user enters a master password and the password generator creates a password based on the master password and the website's URL "on the fly." The disadvantage of password generators is that the browser extension must be installed on each computer and web browser.
- *Online vaults.* An online vault also uses a web browser extension but instead of creating the user's password each time it retrieves the password from a central repository that is online. The disadvantage is that these online sites that store the passwords are vulnerable to attackers.
- *Password management applications.* A password management application is a program installed on a computer through which the user can create and store multiple strong passwords in a single user "vault" file that is protected by one strong master password. Users can retrieve individual passwords as needed by opening the user file, thus freeing the user from the need to memorize multiple passwords. The disadvantage is that the program must be carried with the user or installed on multiple computers.

Most web browsers allow a user to save a password that has been entered while using the browser. However, this feature has several disadvantages. Users can only retrieve passwords on the computer on which they are stored (unless the browser information is synched with other computers). Also, the passwords may be vulnerable if another user is allowed access to their computer. In addition, applications are freely available that allow all of the passwords to be displayed without entering a master password.

Most security experts recommend using a password management application since it provides the highest level of security. These applications also include the additional following features:

- *In-memory protection*. Passwords are "scrambled" while the application is running, so even when the operating system performs functions, it will not reveal any passwords.
- *Key files*. A *key file* is a separate unique file that can be carried on a USB flash drive or other similar device. In order to open the password database, not only must the password be entered, but the key file must also be present. This prevents an attacker who obtains the database password from using it.
- *Lock to user account*. The database can be locked so that it can only be opened by the same person who created it.
- *Import and export*. The password list can be exported to various formats and new passwords can be imported.
- *Random password generator*. A built-in random password generator can create strong random passwords based on different settings like the KeePass generator shown in Figure 2-4.

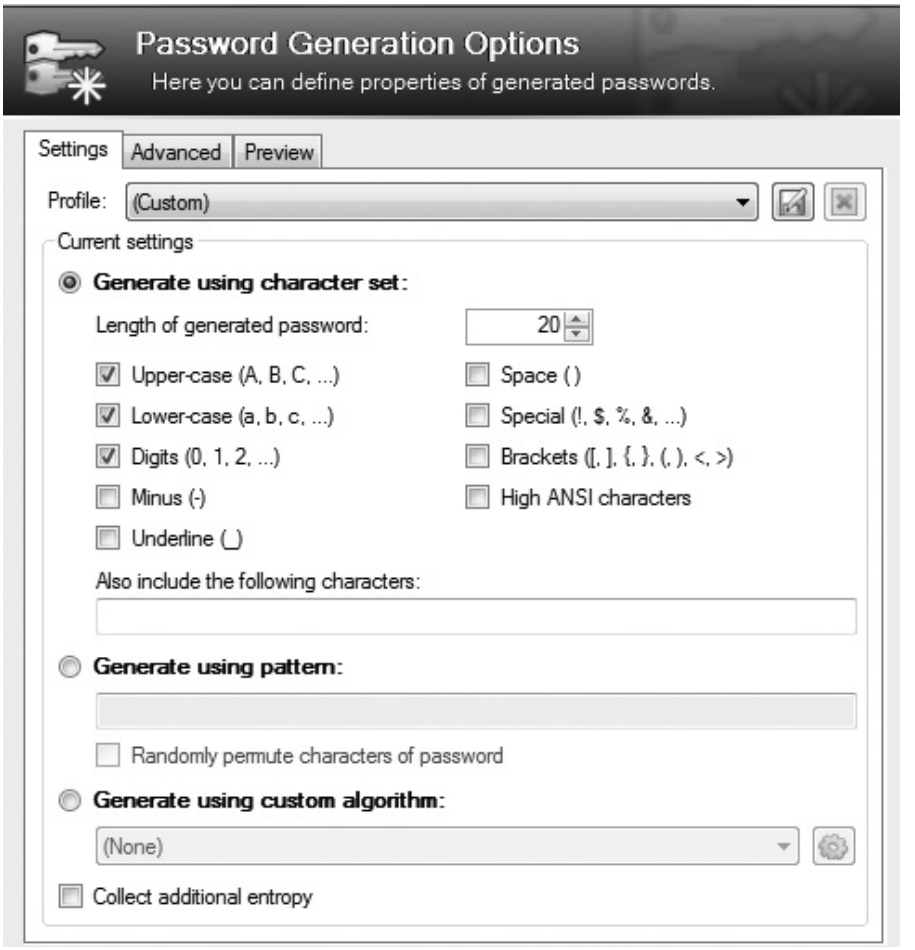


Figure 2-4 KeePass random password generator

Source: KeePass

The value of using a password management application is that unique strong passwords such as *WUuAôxB$2aWøBnd&Tf7MfEtm* can be easily created and used for all accounts.

Despite the value in password managers, most users do not take advantage of them. One recent study compared the responses of security experts against non-experts regarding what they did to stay secure. The results showed that three times more experts than nonexperts reported using password managers for at least some of their accounts (73% vs. 24%), and four times more experts than nonexperts said that using a password manager is one of the most important things they do to stay safe online.[11]

Creating Strong Passwords If a password management application is not used, then **strong passwords** should be created for each separate account. The following general observations regarding creating passwords include:

- Do not use passwords that consist of dictionary words or phonetic words.
- Do not repeat characters (*xxx*) or use sequences (*abc, 123, qwerty*).
- Do not use birthdays, family member names, pet names, addresses, or any personal information.
- Do not use short passwords. A strong password should be a minimum of 18 characters in length.

Passwords should be a long as possible. This is because a longer password is always more secure than a shorter password because the longer a password is, the more attempts an attacker must make in order to try to determine it. The formula for determining the number of possible passwords given the number of characters that can be used in the password and the password length is

Number-of-Keyboard-Keys ^ Password-Length = Total-Number-of-Possible-Passwords.

Table 2-6 illustrates the number of possible passwords for different password lengths using a standard 80-key keyboard. Longer passwords force attackers to spend significantly more time attempting to break them.

Keyboard keys	Password length	Number of possible passwords
80	2	6,400
80	3	512,000
80	4	4,096,000
80	5	3,276,800,000
80	8	1,677,721, 600,000,000

Table 2-6 Number of possible passwords

In technical terms, increasing the length of a password increases the strength *exponentially*, while increasing the complexity will only increase it *linearly*. Because *length is more important than complexity* the password *thisisalongerpassword* is considered stronger than *u$^#16*.

One way to make passwords stronger is to use nonkeyboard characters, or special characters that do not appear on the keyboard. For Microsoft Windows operating systems these characters are created by holding down the *ALT* key while simultaneously typing a number on the numeric keypad (but not the numbers across the top of the keyboard). For example, *ALT + 0163* produces the £ symbol. A list of all the available nonkeyboard characters can be seen by entering *charmap.exe* at the Start screen, and then clicking on a character. The code ALT + 0*xxx* will appear in the lower-left corner of the screen (if that character can be reproduced in Windows). Figure 2-5 shows a Windows character map.

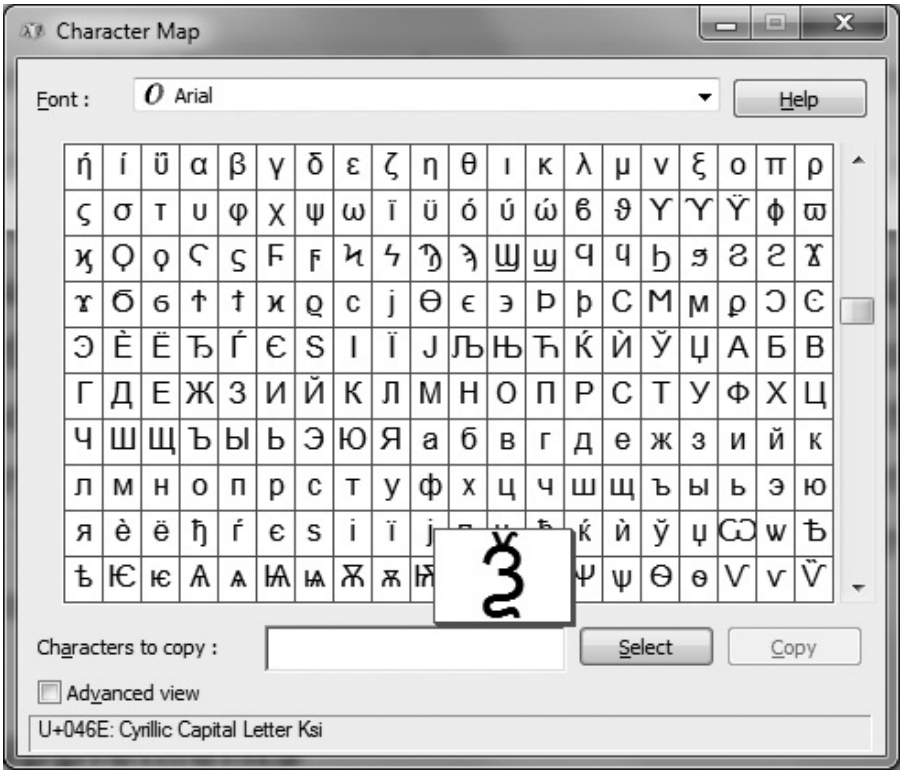


Figure 2-5 Windows character map

Source: Microsoft Windows

Apple has a built-in password generator feature that is often overlooked. When creating a new password, you can click the key icon that is next to the "New Password" field in order to bring up the Apple Password Assistant. The assistant can generate a password based on several choices: Memorable, Letters and Numbers, Numbers Only, Random, or FIPS-181 compliant (FIPS stands for the Federal Information Processing Standards, issued by the National Institute of Standards and Technology). A "Length" slider can set the password length, while a "Quality" indicator gives the strength of your password.

Recognizing Phishing Attacks

Although phishing attacks vary, they generally start with the receipt of an email message that claims to come from a reputable source, such as a bank or website with which the user has an account. The email message may contain the following:

- *Official logos*. Phishers often include the logo of the vendor and otherwise try to make the email look like the vendor's website as a way to convince the recipient that the message is genuine. Yet the presence of logos does not mean that the email is legitimate.
- *Web links*. Phishing emails almost always contain a link that the user is asked to click on. Often these addresses are close variations of a legitimate address, such as *www.ebay_secure.com*, *www.e--bay.com*, or *www.e-baynet.com*.
- *Urgent request*. Most phishing emails encourage the recipient to act immediately or else their account will be deactivated or a similar threatening action will occur shortly.

Even if you carefully scrutinize your email messages, it can be difficult to recognize phishing attacks. The best approach is to consider any unexpected email that claims to come from a reputable source as a phishing message.

You should never click a URL link contained in email message. This is because the link that is displayed (such as *www.ebay.com*) may mask the true link hidden in the message (*such as www.evil.com*).

Avoiding Identity Theft

Identity theft occurs when an attacker uses the personal information of someone else, such as a Social Security number, credit card number, or other identifying information, to impersonate that individual with the intent to commit fraud or other crimes. Avoiding identity theft involves two basic steps. The first step is to deter thieves by safeguarding information. This includes:

- Shred financial documents and paperwork that contains personal information before discarding it.
- Do not carry a Social Security number in a wallet or write it on a check.
- Do not provide personal information either over the phone or through an email message.
- Keep personal information in a secure location in a home or apartment.

The second step is to monitor financial statements and accounts by doing the following:

- Be alert to signs that may indicate unusual activity in an account, such as a bill that did not arrive at the normal time or a large increase in unsolicited credit cards or account statements.
- Follow up on calls regarding purchases that were not made.
- Review financial and billing statements each month carefully as soon as they arrive.

Legislation has been passed that is designed to help U.S. users monitor their financial information. The **Fair and Accurate Credit Transactions Act (FACTA) of 2003** contains rules regarding consumer privacy. FACTA grants consumers the right to request one free credit

report from each of the three national credit-reporting firms every 12 months. If a consumer finds a problem on her credit report, she must first send a letter to the credit-reporting agency. Under federal law, the agency has 30 days to investigate and respond to the alleged inaccuracy and issue a corrected report. If the claim is upheld, all three credit-reporting agencies must be notified of the inaccuracies, so they can correct their files. If the investigation does not resolve the problem, a statement from the consumer can be placed in the file and in any future credit reports.

Because a credit report can only be ordered once per year from each of the credit agencies, it is recommended that one report be ordered every 4 months from one of the three credit agencies. This allows you to view a credit report each quarter without being charged for it.

Setting Social-Networking Defenses

Social-networking sites contain a treasure trove of information for attackers, such as providing information to identity thieves or giving attackers insight into answers to users' security questions that are used for resetting passwords (such as, *What is your mother's maiden name?*). With all of this valuable information available, social-networking sites should be at the forefront of security today; sadly, that is not always the case. Social-networking sites have a history of providing lax security, of not giving users a clear understanding of how security features work, and of changing security options with little or no warning.

There are several general defenses that can be used for any social-networking site. First and foremost, users should be cautious about what information is posted on social-networking sites. Posting *I'm going to Florida on Friday for two weeks* could indicate that a home or apartment will be vacant for that time, a tempting invitation for a burglar. Other information posted could later prove embarrassing. Asking questions such as *Would my boss approve?* Or *What would my mother think of this?* before posting may provide an incentive to rethink the material one more time before posting.

Second, users should be cautious regarding who can view their information. Certain types of information could prove to be embarrassing if read by certain parties, such as a prospective employer. Other information should be kept confidential. Users are urged to consider carefully who is accepted as a friend on a social network. Once a person has been accepted as a friend, that person will be able to access any personal information or photographs. Instead, it may be preferable to show "limited friends" a reduced version of a profile, such as casual acquaintances or business associates.

Finally, because available security settings in social-networking sites are often updated frequently by the site with little warning, users should pay close attention to information about new or updated security settings. New settings often provide a much higher level of security by allowing the user to fine-tune their account profile options.

Table 2-7 lists several privacy and security recommendations for the social-networking site Facebook.

Recommendation	Explanation
Consider how you want to use Facebook	If you only want to keep in touch with people and be able to contact them then you should be more restrictive about what you post and using Facebook functions.
Review the Facebook *Guide to Privacy*	Spend time reading the Facebook *Guide to Privacy*, which contains the latest privacy functions and policies.
Adjust Facebook privacy settings to protect your identity	Facebook provides strong protection options but they must be configured by the user because the default options are usually very permissive.
See your site through the eyes of other users	The *Preview my profile* button on any privacy settings page allows users to check how their information appears to others.
Think carefully about who you allow to become your friend	Once you have accepted someone as your friend they will be able to access virtually any information about you—including photographs—that you have marked as viewable.
Show acquaintances a limited version of your profile	For associates or those with whom you do not want to share all of your information choose to make them acquaintances instead.
Restrict Timeline and Tags	Consider blocking friends from adding to your timeline. Review photos another user attempts to tag you in the Timeline and Tagging Settings by enabling the feature that allows you to review tags people add to your own posts before they appear. Also decide whether tag suggestions should appear when photos that look like you are uploaded.
Disable options, then open them one by one	Disable an option until you have decided you do want and need it, rather than start with everything accessible.

Table 2-7 **Facebook recommendations and explanations**

Exceptional Security

RETAINING DOCUMENTS—There is little need to keep hard copies of select financial documents like bank statements. Most banks provide online access to statements dating back several years that can be accessed as needed. Just keep the last three months of the most recent financial statements and then shred older documents instead of tossing them in the trash or a recycling bin. For paper documents that must be retained, use a scanner to create a PDF of the document and then add a strong password to the PDF file that must be entered before it can be read. Save all the PDF files on a USB flash drive that is stored in a locked file cabinet or a bank safe deposit box. Some local banks offer regular "shred days" when customers can bring in documents to be shredded and destroyed by a licensed document disposal company (but don't just drop off your documents; watch them being shredded). If you are shredding your own documents use a cross-cut shredder and recycle or put the remains in a garden compost pile.

(continues)

MANAGING PASSWORDS—Use a password management application to store all of your passwords on your local computer. Give serious thought to the master password that you will use for this application; make it as long as possible and use some non-keyboard characters. Set up a key file on a USB flash drive so that the application will only open if both your master password is entered and the key file is present. Start by adding your primary accounts to the application and take this opportunity to review the passwords. For any weak passwords use the built-in password generator to create a password that is at least 30 characters in length that is a mix of letters, number, special characters, and brackets. Whenever you are asked to enter a password for an account that is not in your application pause and look at its password and then if necessary generate a new one and store it.

FACEBOOK SECURITY—Periodically check who is accessing your Facebook account. The *Where You're Logged In* section of the Security Settings page displays a list of the browsers and devices that have been used to log in to your Facebook account recently with the date, time, approximate location when signing in, and the type of device used. If you see a *location* that you do not recognize check the *device* to see if you recognize it; when signing in through a mobile device you may be routed through an address that may not actually reflect your physical location. If you think someone else may be logged into your account then terminate the suspicious session. Click *End Activity* (or *Remove* on mobile) next to the session information. Once you end the session, immediately change your Facebook password and record it in your password management application.

Chapter Summary

- When logging in to a computer or a website, users are typically required to provide information that both identifies them and provides proof that they actually are that person. Computers have typically relied upon authenticating users by what they—and no one else—would know. This is done by using a password. A password is a secret combination of letters, numbers, and/or symbols that serves to authenticate a user by what he knows. Despite the fact that passwords are the primary means of authenticating a user, passwords are not considered to be a strong defense against attackers.
- The weakness of passwords centers on human memory. Human beings can only memorize a limited number of items. Long and complex passwords can be difficult to memorize and can strain our ability to accurately recall them. Also, users must remember multiple passwords for many different accounts. Users often take shortcuts and create weak passwords, which compromise security. There are a variety of attacks that can be used to uncover a password. A dictionary attack begins with the attacker creating digests of common dictionary words and then comparing them to those in a stolen password file. This type of attack is successful because users often create passwords that are simple dictionary words. An automated brute force attack uses every possible combination of letters, numbers, and characters to create candidate passwords that are matched to those in the stolen password hash

file. Although slower than a dictionary attack, a brute force attack is more thorough because it tests for all possible passwords. Today attackers use collections of passwords that have stolen from other websites. Because users repeat their passwords on multiple accounts, attackers use these passwords as candidate passwords in their attacks.

- Social engineering is a means of gathering information for an attack by relying on the weaknesses of individuals. It relies on an attacker's clever manipulation of human nature in order to persuade the victim to provide information or take actions. Phishing is sending an email or displaying a web announcement that falsely claims to be from a legitimate enterprise in an attempt to trick the user into surrendering private information. Typo squatting (URL hijacking) takes advantage of user misspellings to direct them to fake websites. Pretexting is creating an invented scenario to persuade the victim to perform an action or provide confidential information. A hoax is a false warning, often contained in an email message claiming to come from an IT department or other authority, and persuades users to take what is claimed to be a protection when in reality it may compromise or infect the system. Dumpster diving involves digging through trash receptacles to find information that can be useful in an attack. Shoulder surfing involves gathering information by observing another person enter the information.
- Identity theft involves using someone's personal information, such as their name, Social Security number, or credit card number to commit financial fraud. Identity theft results in the victim being charged for the purchases as well as a damaged credit history that can be the cause for being turned down for a new job or denied loans for school, cars, and homes.
- The popularity of online social networking has skyrocketed. Social-networking websites link individuals with common interests and function as an online community. While using any website has associated risks, social-networking sites carry additional risks. Personal data posted can be used maliciously. Because social-networking sites by design are intended to share information, these sites have often made it too easy for unauthorized users to view other people's information. To combat this, many sites change their security options on a haphazard basis, making it difficult for users to keep up with the changes.
- The best approach to establishing strong security with passwords is to use a password manager tool. These tools include password generators, online vaults, and password management applications, which are programs that let a user create and store multiple strong passwords in a single user file that is protected by one strong master password. Users can retrieve individual passwords as needed, thus freeing them from the need to memorize multiple passwords. Many password management applications include other tools as well. If a password management application is not used, then strong passwords should be created for each separate account. When creating passwords the most important principle is that length is more important than complexity.
- Although phishing attacks vary, they generally start with the receipt of an email message that claims to come from a reputable source, such as a bank or website with which the user has an account. Despite scrutinizing email messages, it still can be

difficult to recognize phishing attacks. The best approach is to consider any unexpected email that claims to come from a reputable source to be a phishing message.

- Identity theft occurs when an attacker uses the personal information of someone else, such as a Social Security number, credit card number, or other identifying information, to impersonate that individual with the intent to commit fraud or other crimes. Avoiding identity theft involves two basic steps. The first step is to deter thieves by safeguarding information. The second step is to monitor financial statements and accounts.
- There are several defenses that can be used for social-networking sites. Users should be cautious about what information is posted on social-networking sites. Users must also be cautious regarding who can view their information. Users should pay close attention to information about new or updated security settings. It is a good idea to disable options and then enable them only as necessary.

Key Terms

Definitions for key terms can be found in the Glossary for this text.

authentication
brute force attack
dictionary attack
dumpster diving
Fair and Accurate Credit Transactions Act (FACTA) of 2003
hoax
identity theft
password
password manager
phishing
pretexting
shoulder surfing
social engineering
social networking
spear phishing
strong password
typo squatting
username
vishing
weak password
whaling

Review Questions

1. The process of providing proof that the user is "genuine" or authentic is known as _____.
   a. identification
   b. genuinization
   c. authentication
   d. registration
2. Which of the following is NOT a characteristic of a weak password?
   a. personal information in a password
   b. a password with fewer than six characters
   c. a password that uses both letters and numbers
   d. a common dictionary word

3. Relying on deceiving someone to obtain secure information is known as _____.
   a. social engineering
   b. magic attack
   c. brute force attack
   d. sleight attack
4. The goal of a phishing attack is _____.
   a. to capture keystrokes
   b. to send a fraudulent email to a user
   c. to trick a user into surrendering personal information
   d. to duplicate a legitimate service
5. Each of the following may be performed by an identity thief except:
   a. Produce counterfeit checks or debit cards and then remove all money from the bank account.
   b. File for bankruptcy under the person's name to avoid paying debts they have incurred or to avoid eviction.
   c. Open a bank account in the person's name and write bad checks on that account.
   d. Send malware into a bank's online accounting system.
6. Each of the following is a step to deter identity theft except:
   a. Keep personal information in a secure location.
   b. Carry a copy of a Social Security card in a wallet instead of the original.
   c. Shred financial documents that contain personal information.
   d. Do not provide personal information either over the phone or through an email message.
7. Passwords are based on which means of authentication?
   a. what you have
   b. what you do
   c. what you know
   d. what you are
8. A(n) _____ is a unique name for identification.
   a. password
   b. value
   c. authentication
   d. username
9. Each of the following is a characteristic of a strong password except:
   a. It must be lengthy.
   b. It must be easy to memorize.
   c. It must be complex.
   d. It must not be repeated on multiple accounts.

10. Which technique do attackers use today to uncover a password?
    a. online guessing
    b. offline cracking
    c. hash regeneration
    d. digest reproduction
11. Which of these password attacks is the most thorough?
    a. dictionary attack
    b. short crack attack
    c. brute force attack
    d. grill attack
12. Observing someone entering a keypad code from a distance is known as _____.
    a. piggybacking
    b. spoofing
    c. shoulder surfing
    d. cyber watching
13. What is a vishing attack?
    a. an attack that uses a phone instead of email or a website
    b. an attack that only targets "big fish"
    c. a social engineering attack that uses text messages
    d. a password attack designed to crack long passwords
14. A user who enters *americanbank.net* into a web browser instead of the correct *americanbank.com* and is then taken to a fake look-alike site is the victim of _____.
    a. site redirection naming attack (SRNA)
    b. URL targeting
    c. typo squatting
    d. jacket attacking
15. How can an attacker use a hoax?
    a. By sending out a hoax, an attacker can convince a user to read his email more often.
    b. A hoax could convince a user that malware is circulating and that he should change his security settings.
    c. A user who receives multiple hoaxes could contact his supervisor for help.
    d. Hoaxes are not used by attackers today.

16. Michelle pretends to be a manager from another city and calls Eric to trick him into giving her his password. What social-engineering attack has Michelle performed?
    a. pretexting
    b. aliasing
    c. character spoofing
    d. duplicity
17. Why are long passwords stronger than short passwords?
    a. Long passwords are confusing to attackers who cannot read them.
    b. Long passwords require attackers to make many more attempts to uncover the password.
    c. Long passwords always use letters, number, and special characters so they are more puzzling to attackers.
    d. Short passwords take up less storage space which makes them easier to break.
18. Each of the following is a password manager except:
    a. password management application
    b. password generator
    c. online vault
    d. hashing repository
19. Each of the following is typically found in an email used for a phishing attack except:
    a. Official logos of the actual site.
    b. Web links that are close variations of a legitimate address.
    c. An urgent request to take immediate action.
    d. The telephone number of the actual site.
20. Each of the following could be performed in a shoulder surfing attack except:
    a. Watching the victim insert her plastic card into an ATM
    b. Observing a person entering a password on a computer keyboard
    c. Viewing a person writing down his Social Security number on a paper form
    d. Watching a person enter a PIN at a register in a store

Hands-On Projects

Project 2-1: Use an Online Password Cracker

In this project, you will create a digest on a password and then crack it with an online cracking website to demonstrate the speed of cracking passwords.

1. The first step is to use a hash algorithm to create a password digest. Use your web browser to go to **www.fileformat.info/tool/hash.htm** (if you

are no longer able to access the site through the web address, use a search engine to search for "Fileformat.Info hash functions").

2. Under **String hash**, enter the simple password **apple123** in the **Text:** line.
3. Click **Hash**.
4. Scroll down the page and copy the MD4 hash of this password to your Clipboard by selecting the text, right-clicking, and choosing **Copy**.
5. Open a new tab on your web browser.
6. Go to **https://crackstation.net/**.
7. Paste the MD4 hash of *apple123* into the text box beneath **Enter up to 10 non-salted hashes:**.
8. In the RECAPTCHA box, enter the current value being displayed in the box that says **Type the text**.
9. Click **Crack Hashes**.
10. How long did it take this online rainbow table to crack this hash?
11. Click the browser tab to return to FileFormat.Info.
12. Under **String hash**, enter the longer password **12applesauce** in the **Text:** line.
13. Click **Hash**.
14. Scroll down the page and copy the MD4 hash of this password to your Clipboard.
15. Click to browser tab to return to the CrackStation site.
16. Paste the MD4 hash of *12applesauce* into the text box beneath **Enter up to 10 non-salted hashes:**.
17. In the RECAPTCHA box, enter the current value being displayed in the box that says **Type the text**.
18. Click **Crack Hashes**.
19. How long did it take this online rainbow table to crack this stronger password hash?
20. Click the browser tab to return to FileFormat.Info and experiment by entering new passwords, computing their hash, and testing them in the CrackStation site. If you are bold, enter a string hash that is similar to a real password that you use.
21. What does this tell you about the speed of cracking passwords? What does it tell you about how easy it is for attackers to crack weak passwords?
22. Close all windows.

Project 2-2: Download and Install a Password Management Application

The drawback to using strong passwords is that they can be very difficult to remember, particularly when a unique password is used for each account that a user has. As another option, password management applications allow users

to store account information such as a username and password. These programs are themselves protected by a single strong password. One example of a password storage application is KeePass Password Safe, which is an open-source product. In this project, you will download and install KeePass.

1. Use your web browser to go to **keepass.info** and then click **Downloads** (if you are no longer able to access the site through the web address, use a search engine to search for "KeePass").
2. Under **Professional Edition**, locate the most recent portable version of KeePass and click it to download the application. Save this file in a location such as your desktop, a folder designated by your instructor, or your portable USB flash drive. When the file finishes downloading, install the program. Accept the installation defaults.

Because this is the portable version of KeePass it does not install under Windows. In order to use it, you must double-click the filename KeePass.exe.

3. Launch KeePass to display the opening screen.
4. Click **File** and **New** to start a password database. Enter a name for the password database and save it to your computer. Enter a strong master password for the database to protect all of the passwords in it. Enter the password again in the Repeat password box. Then, click **OK** twice.
5. Click **Edit** and **Add Entry**. You will enter information about an online account that has a password that you already use. Click **OK** when you are finished.
6. Create a group by clicking **Edit** and then **Add Group** and then enter **Web Sites**. Click **OK** when you are finished.
7. Select the **Web Sites** group and click **Edit** and then **Add Entry**.
8. Enter a title for your website (such as *Google Gmail*) under **Title**.
9. Under **User name**, enter the username that you use to log in to this account.
10. Erase the entries under **Password** and **Repeat** and enter the password that you use for this account and confirm it.
11. Enter the URL for this account under **URL**.
12. Click **OK**.
13. Click **File** and **Save**.
14. Exit KeePass.
15. If necessary, navigate to the location of KeePass and double-click the file **KeePass.exe** to launch the application.
16. Enter your master password to open your password file.

17. If necessary, click the group to locate the account you just entered; it will be displayed in the right pane.
18. Click the link next to the URL to go to that website.
19. Click KeePass in the taskbar so that the window is now on top of your browser window.
20. Drag and drop your username from KeePass into the login username box for this account in your web browser.
21. Drag and drop your password from KeePass for this account.
22. Click the button on your browser to log in to this account.
23. Because you can drag and drop your account information from KeePass, you do not have to memorize any account passwords and can instead create strong passwords for each account. Is this an application that would help users create and use strong passwords? What are the strengths of such password programs? What are the weaknesses? Would you use KeePass?
24. Close all windows.

Project 2-3: Download and Install an Online Vault Password Manager

One of the drawbacks to using a password management program like KeePass is that it must be launched whenever a password must be retrieved or the program must be left open, which could be a security risk. An option is to use a browser-based online vault password manager program that retrieves the passwords automatically. One example of a browser-based password storage program is LastPass, which enables you to access your passwords from any computer. In this project, you will download and install LastPass.

1. Use your web browser to go to **lastpass.com** and click **Download Free** (if you are no longer able to access the site through the web address, use a search engine to search for "LastPass").
2. Click **Watch screencast tutorials to learn the basics**.
3. Click **Getting started with LastPass** to open the tutorial screen, and if necessary click the **Play** button in the middle of the screen.
4. When the Basic Instructions tutorial has completed, click your browser's **Back** button.
5. Click **Watch screencast tutorials to learn the basics** again.
6. Click **How to Automatically Fill Webpage Forms** to open the tutorial screen, and if necessary click the **Play** button in the middle of the screen.
7. When the tutorial has completed, click your browser's **Back** button.
8. Click the **Download** button to download LastPass.

9. After the program has downloaded, launch the program and follow the instructions for the default installation.
10. Under **Create or Log In** be sure to click **Create a New Account.**
11. Enter your email address and create a password. Be sure to remember this information.
12. Accept the default settings to finish installing and creating your LastPass account.

The steps may vary for installing LastPass depending upon which web browser you are using.

13. Close your web browser.

Project 2-4: Using a Browser-Based Password Management Program

In this project, you will use the LastPass program installed in the previous project.

1. Launch your web browser. If necessary, enable the LastPass browser extension.
2. Notice that you now have a LastPass button at the top of the screen. Click **LastPass**.
3. Enter your Master Password and then click **Login**.
4. Point your web browser to a website you frequently use that requires you to enter your username and password.
5. Enter your username and password. Notice that LastPass now asks if you want it to remember this password. Click **Save Site**.
6. When the **Add Site** window opens, click **Save**.
7. Log out of the website.
8. Now log in to two other websites and record their passwords in LastPass.
9. Close the web browser.
10. Reopen the web browser and click the **LastPass** icon on the toolbar. Notice that you are still logged in.
11. Click the **LastPass** icon and select the site that you want to visit. What happens when you go to these sites?

Your LastPass passwords can be retrieved from any other computer's web browser that has LastPass installed; you are not restricted to only this computer.

12. Because your login information automatically appears in LastPass, you do not have to memorize any account passwords and can instead create strong passwords for each account. Is this an application that would help users create and use strong passwords? What are the strengths of browser-based password program? What are the weaknesses? How does LastPass compare to KeePass? Would you use LastPass?
13. Close all windows.

Project 2-5: Download and Install a Password Generator

Another option to password managers is browser extensions that generate passwords. Instead of storing user-created passwords, these extensions transparently combine multiple elements (such as the username, master password, and site's domain name) into a single site-specific password. The user begins by entering their username and master password, and then the extension generates their site-specific password. The remote site only sees a domain-specific digest instead of the master password itself. In this project you install and use SuperGenPass.

1. Use your web browser to go to **supergenpass.com** (if you are no longer able to access the site through the web address, use a search engine to search for "SuperGenPass").
2. Drag the icon **SGP** to your browser's bookmarks toolbar.
3. Click **SGP** on your browser's bookmarks toolbar to launch the SuperGenPass dialog box as displayed in Figure 2-6.

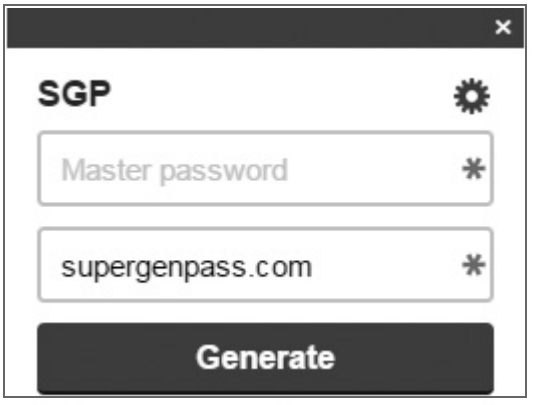


Figure 2-6 SuperGenPass dialog box

Source: SuperGenPass

4. Think of a strong Master Password for SGP but do not enter it yet.
5. Now create an account that requires a password. Go to **gmx.com**.
6. Click **Sign up**.

7. Enter the requested information to create an account. When prompted for a password do not enter a password in GMX but instead click **SGP** in your browser's bookmarks toolbar.
8. Enter your strong **Master password** in the SGP dialog box.
9. Click **Generate.** Note that the password is automatically entered into the password fields.
10. Enter the remaining personal information on the form and create your GMX email account.
11. If necessary, click the **Continue to inbox** button. Click **Log out** to exit your GMX email account.
12. Now access your GMX account with SuperGenPass entering your password. Go to *gmx.com*.
13. Click **Log In**.
14. Enter your email address in the Email box.
15. Click **SGP**.

If nothing happens when you click SGP, you might need to switch to a different browser.

16. The SuperGenPass dialog box opens. Enter your master password created above.
17. Click **Generate.**
18. Click **Log in**.
19. Note that you have entered the website without the need to memorize a unique password for each site.
20. Click **Log out** to exit your GMX email account.
21. How would you rate SuperGenPass compared to KeePass? How does it compare to LastPass? Which of these do you consider the most convenient to use?
22. Close all windows.

Project 2-6: Viewing Your Annual Credit Report

Security experts recommend that consumers receive a copy of their credit report at least once per year and check its accuracy to protect their identity. In this project, you will access your free credit report online.

1. Use your web browser to go to **www.annualcreditreport.com**. Although you could send a request individually to one of the three credit agencies, this website acts as a central source for ordering free credit reports. Figure 2-7 shows the website.
2. Click **Request your free credit reports**.
3. Click **Request your credit reports.** Enter the requested information and click **Next**.
4. Click **TransUnion**. Click **Next**.

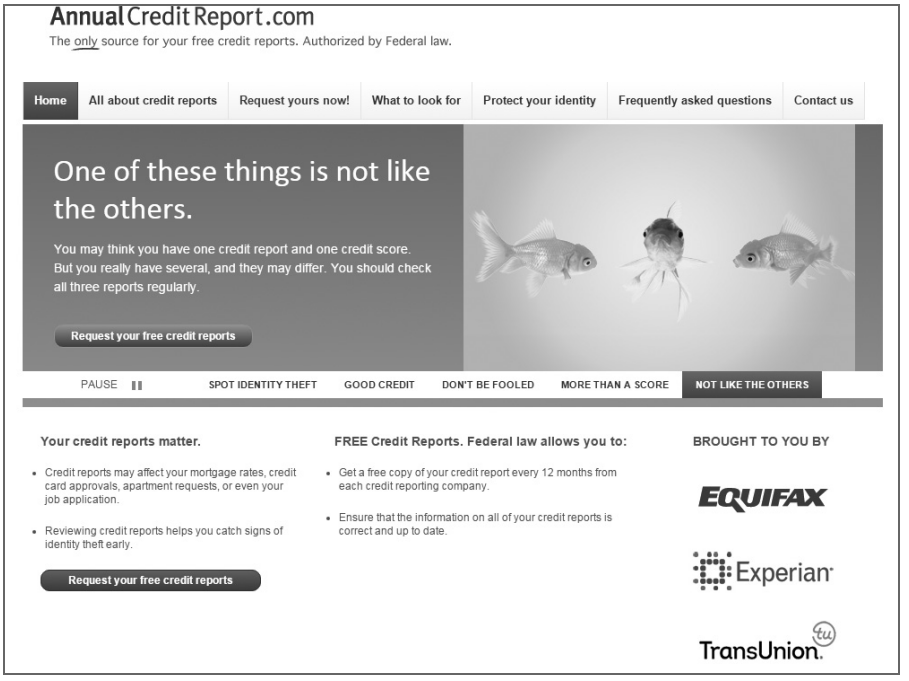


Figure 2-7 Credit report website

Source: Annual Credit Report

5. Click **Continue**.
6. You may then be asked personal information about your transaction history in order to verify your identity. Answer the requested questions.
7. Follow the instructions to print your report. Review it carefully, particularly the sections of "Potentially negative items" and "Requests for your credit history." If you see anything that might be incorrect, follow the instructions on that website to enter a dispute.
8. Follow the instructions to exit from the website.
9. Close all windows.

Case Projects

Case Project 2-1: Testing Password Strength

How strong are your passwords? Various online tools can provide information on password strength, but not all feedback is the same. First, assign the numbers 1 through 3 to three of the passwords you are currently using, and write down the number (not the password) on a piece of paper. Then, enter those passwords into these three online password testing services:

- How Secure Is My Password (*howsecureismypassword.net/*)

- Check Your Password (*www.microsoft.com/security/pc-security/password-checker.aspx*)
- The Password Meter (*www.passwordmeter.com/*)

Record next to each number the strength of that password as indicated by these three online tools. Then use each online password tester to modify the password by adding more random numbers or letters to increase its strength. How secure are your passwords? Would any of these tools encourage someone to create a stronger password? Which provided the best information? Create a one-paragraph summary of your findings.

Case Project 2-2: Information Security Community Site Activity

The Information Security Community Site is an online companion to this textbook. It contains a wide variety of tools, information, discussion boards, and other features to assist learners. Go to *community.cengage.com/infosec*. Sign in with the login name and password that you created in Chapter 1.

Take the challenge to convince three of your friends that they must strengthen their passwords. Create a script of what you will say to them in an attempt to convince them of the dangers of weak passwords and the seriousness of the problem, and to inform them about what practical solutions are available. Then approach each friend individually and see whether you can be successful. Make a record of their responses and reactions to stronger passwords.

Record what occurred on the Community Site discussion board. What did you learn from this? How hard or easy is it to challenge users to create strong passwords? What arguments did you hear against it? What helped convince them to create stronger passwords?

Additional Case Projects for this chapter are available through the MindTap online learning environment.

References

1. Vu, K.-P., Proctor, R., Bhargav-Spantzel, A., Tai, B.-L., Cook, J., and Schultz, E., "Improving Password Security and Memorability to Protect Personal and Organizational Information." *International Journal of Human-Computer Studies*, *65*, 744–57.
2. Sasse, M., and Brostoff, S. W., "Transforming the 'Weakest Link': A Human/Computer Interaction Approach to Usable and Effective Security." *BT Technology Journal*, *19*(3), 122–31.
3. Bennett, Shea, "Average User Has 5.54 Social Media Accounts, Says Study." *Social Times*. Jan. 26, 2015. Retrieved August 5, 2015, http://www.adweek.com/socialtimes/average-number-social-networks/613431.
4. Schneier, Bruce, *Secrets and Lies: Digital security in a Networked World* (New York: Wiley Computer Publishing), 2004.

5. Goodin, Dan, "25-GPU Cluster Cracks Every Standard Windows Password in <6 Hours," *ARS Technica*, Dec. 9, 2012. Retrieved Apr. 3, 2014, http://arstechnica.com/security/2012/12/25-gpu-cluster-cracks-every-standard-windows-password-in-6-hours/.
6. McNichol, Tom, "Friend Me on Faecbook," *Bloomberg Businessweek*. Nov. 7, 2011.
7. Gee, Garrett, and Kim, Peter, "Doppelganger Domains." *GodaiGroup*. September 6, 2011. Accessed Jan. 7, 2014. http://files.godaigroup.net/wp-content/uploads/doppelganger/Doppelganger.Domains.pdf.
8. Fram, Alan, "IRS Taking Steps to Combat Taxpayers' Identity Theft." *The Seattle Times*. June 11, 2015. Retrieved Aug. 5, 2015. http://www.seattletimes.com/nation-world/nation-politics/irs-taking-steps-to-combat-taxpayers-identity-theft/.
9. Rubin, Richard and Gambrell, Dorothy, "Ripping Off Uncle Sam." *Bloomberg Business*. Retrieved Aug. 5, 2015. http://www.bloomberg.com/graphics/2015-web-comic-irs-tax-fraud/
10. "Number of Monthly Active Facebook Users Worldwide as of 2nd Quarter 2015 (in millions)." *Statista*. Retrieved Aug. 5, 2015. http://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/.
11. Ion, Iulia, Reeder, Rob, and Consolvo, Sunny, " '... No One Can Hack My Mind': Comparing Expert and Non-Expert Security Practices.", *2015 Symposium on Usable Privacy and Security*. July 22–24, 2015. Retrieved Aug. 7, 2015. https://www.usenix.org/system/files/conference/soups2015/soups15-paper-ion.pdf

chapter 3

Computer Security

After completing this chapter you should be able to do the following:

- Define malware
- List the different types of malware
- Identify payloads of malware
- Describe the steps for securing software
- Explain how to create data backups

Security in Your World

"Excuse me, Dr. Antonelli. Do you have a minute?" Dr. Antonelli looked up from his computer. "Hi, Sanne. Yes, please come in." Sanne was taking an Introduction to Modern Technology course taught by Dr. Antonelli at the college, who also taught upper-level security courses. "I wanted to get your advice on something, and I knew you were the one to talk with," she said. Dr. Antonelli cleared off some papers from a chair. "Have a seat. What can I help you with? Something about our class?"

Sanne sat down in the chair and opened her backpack. "No, our class is going fine. At least until next week's exam!" Dr. Antonelli laughed. "You are doing just fine in this class. I just wish some of your classmates were as dedicated as you are!" Sanne grinned. "Thank you. Anyway, my Uncle Brian has been overseas on a consulting job for the past year and just got back home. Since he missed my birthday he had told me that he wanted to give me a nice gift when he got back. He just brought it over yesterday. It's a new computer. See?" Sanne handed the device to her teacher. "This is really nice, Sanne. It's one of those convertible models that you can use as either a laptop or as a tablet device. And it's so light. You will really enjoy this," said Dr. Antonelli.

"Thanks," said Sanne. "What I wanted to ask you was what I should have on this computer to protect it. I know that you teach security courses and I thought you could tell me what I needed to keep it from getting infected. My mother and brother both say that all I need is antivirus software. But after our class last week I don't think so. What would you do to protect it?" she asked.

Dr. Antonelli handed the device back to Sanne. "It's interesting that you should ask. I just read an article that asked over 200 security experts what they did to protect their computers and compared that with what non-experts said. The results were very different between the two groups," he said as he pulled a copy of the article out of his backpack. "Look. It says that 42 percent of the non-experts responded that antivirus software was one of the top three protections you should have. But among the security experts, installing antivirus software did not even make the list. And only 7 percent of all the experts even said that antivirus software was important."

Sanne looked at the paper Dr. Antonelli was holding. "Wow, that's a huge difference. So security experts say that antivirus is not that important but most users think that it is. Why do they think that?" she asked. Dr. Antonelli leaned back. "The authors of this journal article speculated that antivirus software offers a convenient install-and-forget type of solution that's very easy for users to manage. That's probably true. I also think that most users consider all attacks as coming from 'viruses' so they believe 'antivirus' then repels everything. But there are many different types of attacks against computers today besides viruses."

Sanne looked at Dr. Antonelli and asked, "So what are these other attacks?"

Protecting your personal technology device—be it a desktop, laptop, or tablet—is a challenge, even for the most advanced computer users. This is because many different types of attacks are launched against personal technology devices, and attackers are constantly modifying these attacks as well as creating new ones daily. According to a major security vendor, malicious software "events" directed at a business enterprise occur on average once every three minutes.[1]

Although virtually every computer user wishes for a single defensive program or one configuration setting that would fully protect their equipment, none exists. Just as a house must be protected against different types of threats—burglary, arson, vandalism, hurricanes, mold, and termites—so too must a computer be protected from a variety of attacks. And just as protecting against termites is much different than protecting against a hurricane, there are several different defenses that must be in place for a computer to remain safe.

In this chapter, you will learn about computer security. You will start by looking at the types of computer attacks that occur today. And then you will find out what defenses must be in place to keep our computers and the information stored on them secure.

Attacks Using Malware

Malware is software that enters a computer system without the user's knowledge or consent and then performs an unwanted and usually harmful action. Strictly speaking, malware uses a threat vector to deliver a malicious "payload" that performs a harmful function once it is invoked. However, *malware* is most often used as a general term that refers to a wide variety of damaging software programs.

Different types of malware have emerged over time as a result of security defenses becoming more sophisticated and the corresponding attacks becoming progressively more complex. However, there has been no standard established for the classification of the different types of malware. As a result, the definitions of the different types of malware are often confusing and may overlap. One method of classifying the various types of malware is by using the primary trait that the malware possesses. These traits are circulation, infection, concealment, and payload capabilities.

In order to detect malware on an infected computer, a software scanning tool can search for the malware, looking to match it against a known pattern of malicious software. To circumvent this detection of their software, attackers have become very sophisticated at masking the presence of their malware by having it "mutate" or change.

Circulation/Infection

Some malware has as its primary trait spreading rapidly to other systems in order to impact a large number of users. Malware can circulate through a variety of means: by using the network to which all the devices are connected, through USB flash drives that are shared

among users, or by sending the malware as an email attachment. Some malware attaches itself to a benign program while other malware functions as a stand-alone process. Once the malware reaches a system through circulation, it must "infect" or embed itself into that system. Three types of malware have the primary traits of circulation and/or infection. These are viruses, worms, and Trojans.

Viruses A biological virus is an agent that reproduces inside a cell. When a cell is infected by a virus, the virus takes over the operation of that cell, converting it into a virtual factory to make more copies of it. The cell is forced to produce thousands or hundreds of thousands of identical copies of the original virus very rapidly (the polio virus can make more than *one million* copies of itself inside one single infected human cell). Biologists often say that viruses exist only to make more viruses. A **computer virus** (**virus**) is malicious computer code that, like its biological counterpart, reproduces itself on the same computer. Strictly speaking, a computer virus replicates itself (or an evolved copy of itself) without any human intervention.

Sometimes the terms *virus* and *malware* are used synonymously, especially by the general news media when reporting on a security incident. However, this is incorrect: a virus is only one type of malware.

Almost all viruses "infect" by inserting themselves into a computer file. A large number of different file types can contain a virus; for example, over 70 different Microsoft Windows file types can be infected. A virus that infects an executable program file is simply called a *program virus*. When the program is launched the virus is activated. A virus can also infect a data file like a Microsoft Office document or spreadsheet. One of the most common data file viruses is a *macro virus* that is written in a script known as a macro. A *macro* is a series of instructions that can be grouped together as a single command. Often macros are used to automate a complex set of tasks or a repeated series of tasks and are stored within the user document (such as in an Excel .XLSX worksheet or Word .DOCX file). Once the document is opened the macro instructions then execute whether those instructions are benign or a macro virus.

One of the first viruses found on a personal computer was written for the Apple II in 1982. Rich Skrenta, a ninth-grade student in Pittsburgh, wrote "Elk Cloner," which displayed his poem on the screen after every 50th use of the infected floppy disk. Unfortunately, the virus leaked out and found its way onto the computer used by Skrenta's math teacher.[2] In 1984, the mathematician Dr. Frederick Cohen introduced the term *virus* based on a recommendation from his advisor, who came up with the name from reading science fiction novels.

Early viruses were relatively straightforward in how they infected files. One basic type of infection is the *appender infection*. The virus first attaches or appends itself to the end of the infected file. It then inserts at the beginning of the file a "jump" instruction that points to the end of the file, which is the beginning of the virus code. When the program is

launched, the jump instruction redirects control to the virus. Figure 3-1 shows how an appender infection works.

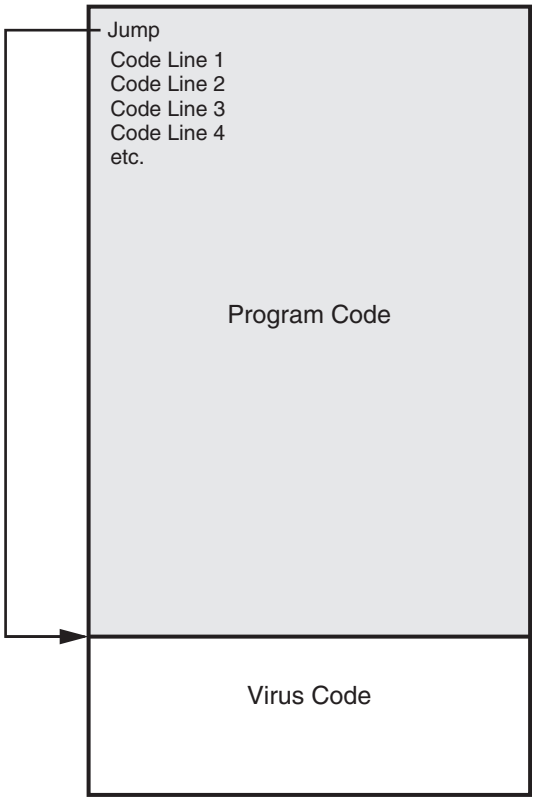


Figure 3-1 Appender infection

However, these types of viruses could easily by detected by software scanning for a virus. Most viruses today go to great lengths to avoid detection. One of the more sophisticated types of virus uses a *split infection*, which divides the malicious code itself into several parts (along with one main body of code), and then these parts are placed at random positions throughout the program code. To make detection even more difficult, these parts may contain unnecessary "garbage" code to mask their true purpose. A split infection virus is shown in Figure 3-2.

Some viruses even scan for the presence of files that security researchers typically use. If those files are present, then it is assumed that the virus is being examined for weaknesses. The virus will then automatically self-destruct by deleting itself or cripple the computer so that it can no longer be used.

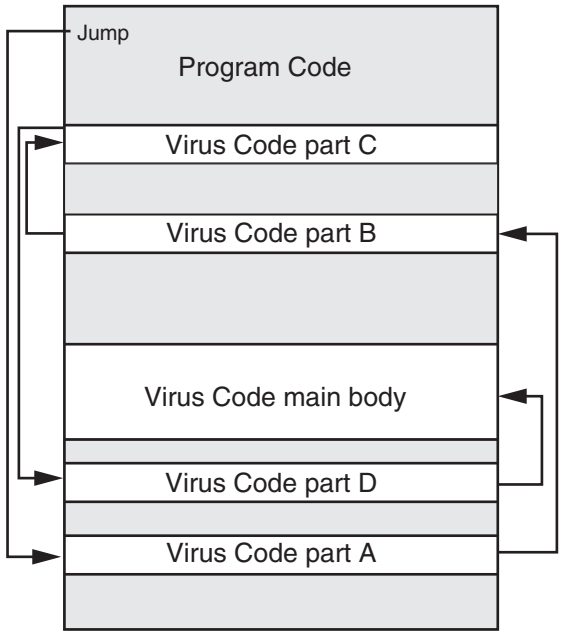


Figure 3-2 Split infection

Each time the infected program is launched or the file is opened—either by the user or the computer's operating system—the virus performs two actions. First, it unloads a payload to perform a malicious action. Although early viruses often did nothing more than display an annoying message, viruses today are much more harmful. Viruses have performed the following actions:

- Caused a computer to crash repeatedly
- Erased files from a hard drive
- Turned off the computer's security settings
- Reformatted the hard disk drive

Sometimes a virus will remain dormant for a period of time before unleashing its payload.

The second action a virus takes when executed is to reproduce by inserting its code into another file on the same computer. A virus can only replicate on the host computer on which it is located; it cannot automatically spread to another computer by itself. Instead, it must rely on the actions of users to spread to other computers. Because viruses are generally attached to files, viruses are spread by a user transferring those files to other devices. For example, a user may send an infected file as an email attachment or copy

an infected file to a USB flash drive and give the drive to another user. Once the virus reaches a new computer it begins to infect it. This means that a virus must have two "carriers": a file to which it attaches and a human to email or transport it to other computers.

Several similarities between biological and computer viruses exist: both must enter their host passively (by relying on the action of an outside agent), both must be on the correct host (a horse virus cannot make a human sick, just as an Apple Mac virus cannot infect a Windows computer), both can only replicate when inside the host, both may remain dormant for a period of time, and both types of viruses replicate at the expense of the host.

Worms A second type of malware that has as its primary purpose to spread is a worm. A **worm** is a malicious program that uses a computer network to replicate (worms are sometimes called *network viruses*). A worm is designed to enter a computer through the network and then take advantage of a vulnerability in an application or an operating system on the host computer. Once the worm has exploited the vulnerability on one system, it immediately searches for another computer on the network that has the same vulnerability.

One of the first wide-scale worms occurred in 1988. This worm exploited a misconfiguration in a program that allowed commands emailed to a remote system to be executed on that system, and it also carried a payload that contained a program that attempted to determine user passwords. Almost 10 percent of the devices connected to the Internet at that time were affected. The author of the worm was later convicted of federal crimes in connection with this incident.

Early worms were relatively harmless and designed simply to spread quickly and not corrupt the systems they infected. These worms slowed down the network through which they were transmitted by replicating so quickly that they consumed all network resources. Today's worms can leave behind a payload on the systems they infect and cause harm, much like a virus. Actions that worms have performed include:

- Deleting files on the computer
- Allowing the computer to be remotely controlled by an attacker.

Although viruses and worms are said to be automatically self-replicating, *where* they replicate is different. A virus will self-replicate *on* the host computer but not to other computers. A worm will self-replicate *between* computers (from one computer to another).

Trojans According to ancient legend, the Greeks won the Trojan War by hiding soldiers in a large hollow wooden horse that was presented as a gift to the city of Troy. Once the

horse was wheeled into the fortified city, the soldiers crept out of the horse during the night and attacked the unsuspecting defenders.

A computer **Trojan horse** (or just **Trojan**) is an executable program that masquerades as performing a benign activity but also does something malicious. For example, a user may download what is advertised as a calendar program, yet when it is installed, in addition to installing the calendar it installs malware that scans the system for credit card numbers and passwords, connects through the network to a remote system, and then transmits that information to the attacker.

Unlike a virus that infects a system without the user's knowledge or consent, a Trojan program is installed on the computer system with the user's knowledge. What the Trojan conceals is its malicious payload.

Table 3-1 lists the differences between viruses, worms, and Trojans.

Action	Virus	Worm	Trojan
What does it do?	Inserts malicious code into a program or data file	Exploits a vulnerability in an application or operating system	Masquerades as performing a benign action but also does something malicious
How does it spread to other computers?	User transfers infected files to other devices	Uses a network to travel from one computer to another	User transfers Trojan file to other computers
Does it infect a file?	Yes	No	It can
Does it require user action to spread?	Yes	No	Yes

Table 3-1 Difference between viruses, worms, and Trojans

Concealment

Some types of malware have avoiding detection as a primary trait. A **rootkit** is a set of software tools used to hide the actions or presence of other types of software, such as Trojans, viruses, or worms. Rootkits do this by changing the operating system to force it to ignore their malicious files or activity. Rootkits also hide or remove all traces of evidence that may reveal the malware, such as log entries.

One approach used by rootkits is to alter or replace operating system files with modified versions that are specifically designed to ignore malicious evidence. For example, antimalware scanning software may be instructed to examine all files in a specific directory. In order to do this, the scanning software receives a list of those files from the operating system. A rootkit replaces the operating system's program that creates an accurate list of files with the rootkit's own routine that creates a list of files but omits any malicious files from the list. This is illustrated in Figure 3-3. The scanning software assumes that the operating system

will willingly carry out those instructions and retrieve all files; it does not know that the computer is providing only files that the rootkit has approved. In essence, users can no longer trust their computer that contains a rootkit: the rootkit is in charge and hides what is occurring on the computer.

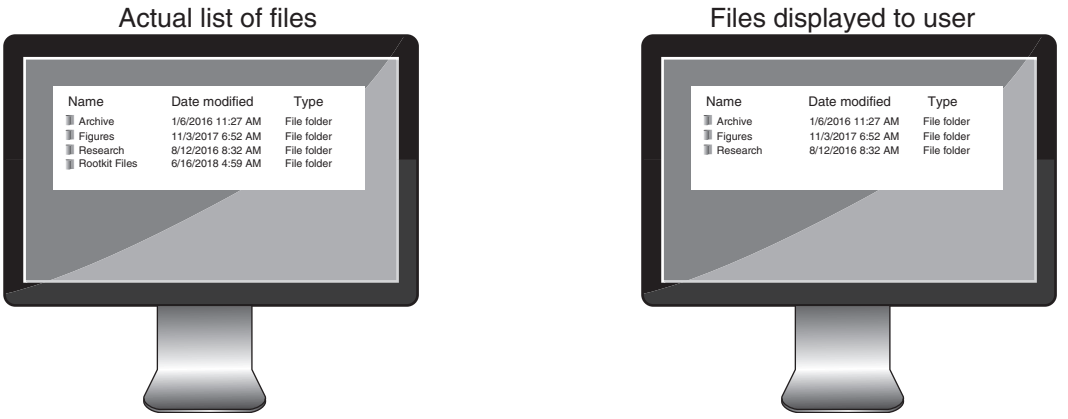


Figure 3-3 Computer infected with rootkit

Because a rootkit often substitutes its own malicious files and routines for legitimate operating system files, it can be very difficult to detect the presence of a rootkit; the operating system cannot be trusted to provide accurate information. In addition, these files and routines typically operate at a very low level in the operating system and cannot easily be repaired. Ultimately, the only safe and foolproof way to handle a rootkit infection is to reformat the hard drive and reinstall the operating system.

Payload Capabilities

When payload capabilities are the primary emphasis of malware, the focus is on what nefarious action(s) the malware performs. Does it allow the attacker to execute commands on the remote computer or to steal passwords and other valuable data from the user's system? Does it delete programs so the computer can no longer function properly? Or does the malware modify the system's security settings? And in some cases the purpose of this malware is to use the infected system to launch attacks against other computers. The primary payload capabilities are to execute commands, collect data, delete data, modify system security settings, and launch attacks.

Execute Commands When the payload allows an attacker to execute virtually any command on the victim's computer this is called **arbitrary code execution**. Most often arbitrary code execution takes advantage of a vulnerability in the operating system software or an application program. The attacker uses a relatively small piece of computer code called *shellcode* as the payload. The shellcode launches ("spawns") a command

shell from which instructions can then be issued to the computer. When malware can trigger arbitrary code execution on Computer A remotely from Computer B over a network or the Internet, this is called **remote code execution**.

Many shellcode snippets are freely available for download. A small portion of shellcode would appear as *\xda\xde\xd9\x74\x24\xf4\xb8\x22\xd2\x27\x7a\x29 \xc9\xb1\x4b*.

Collect Data Different types of malware are designed to collect important data from the user's computer and make it available at the attacker. This malware includes spyware, adware, and ransomware.

Spyware **Spyware** is a general term used to describe software that secretly spies on users by collecting information without their consent. The Anti-Spyware Coalition defines spyware as tracking software that is deployed without adequate notice, consent, or control by the user.[3] This software uses the computer's resources, including programs already installed on the computer, for the purpose of collecting and distributing personal or sensitive information. Table 3-2 lists different technologies used by spyware.

Technology	Description	Impact
Automatic download software	Used to download and install software without the user's interaction	May be used to install unauthorized applications
Passive tracking technologies	Used to gather information about user activities without installing any software	May collect private information such as websites a user has visited
System modifying software	Modifies or changes user configurations, such as the web browser home page or search page, default media player, or lower-level system functions	Changes configurations to settings that the user did not approve
Tracking software	Used to monitor user behavior or gather information about the user, sometimes including personally identifiable or other sensitive information	May collect personal information that can be shared widely or stolen, resulting in fraud or identity theft

Table 3-2 Technologies used by spyware

Not all spyware is necessarily malicious. For example, spyware monitoring tools can help parents keep track of the online activities of their children while the children are surfing the web.

One type of nefarious spyware is a **keylogger** that silently captures and stores each keystroke that a user types on the computer's keyboard. The attacker then searches the captured text for any useful information such as passwords, credit card numbers, or personal information.

A keylogger can be a small hardware device or a software program. As a hardware device, the keylogger is inserted between the computer keyboard connection and USB port, as shown in Figure 3-4. Because the device resembles an ordinary keyboard plug and the computer keyboard USB port is often on the back of the computer, a hardware keylogger can easily go undetected. In addition, the device is beyond the reach of the computer's antimalware scanning software and thus raises no alarms. The attacker who installed the hardware keylogger returns at a later time and physically removes the device in order to access the information it has gathered.

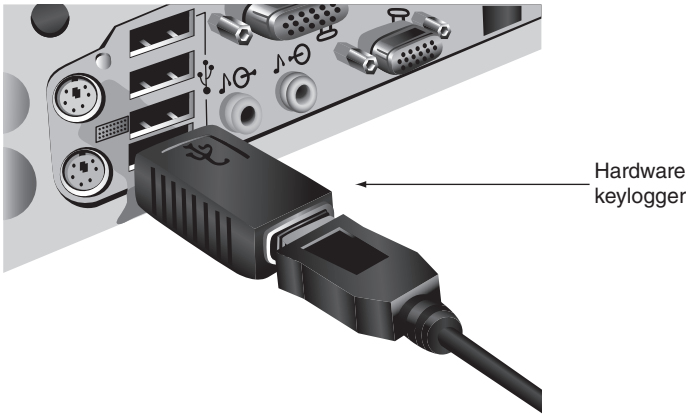


Figure 3-4 Hardware keylogger

Today's hardware keyloggers have several advanced features. Some keyloggers will wirelessly transmit the captured information so that the user does not have to return and physically remove the device. Other keyloggers can be embedded into the keyboard itself and are completely invisible. The storage capacities of the hardware keyloggers can reach into the millions of keystrokes, thus capturing up to an entire year's worth of information.

Software keyloggers are programs installed on the computer that silently capture keystrokes. These programs act like rootkits and conceal themselves so that they cannot be easily detected by the user. An advantage of software keyloggers is that they do not require physical access to the user's computer as with a hardware keylogger. The software, often installed as a Trojan or by a virus, can routinely send captured information back to the attacker through the computer's Internet connection. Yet today's software keyloggers go far beyond just capturing a user's keystrokes: these programs can also make screen captures of everything that is on the user's screen and silently turn on the computer's web camera to record images of the user.

Keyloggers are often installed on public access computers, such as those in a school's open computer lab or a public library. If a sensitive password must be entered on one of these computers, almost all operating systems offer an on-screen "virtual" keyboard through which the keys are clicked with a mouse or touch screen, thus defeating a keylogger. For Windows computers it is found by clicking Accessories and then Ease of Use.

Adware **Adware** collects user information and then delivers advertising content in a manner that is unexpected and unwanted by the user. This is because adware programs essentially perform a tracking function, which monitors and tracks a user's online activities. It then sends a log of these activities to third parties—without the user's authorization or knowledge—who deliver their ads to the user.

Once the adware malware becomes installed, it typically displays advertising banners, popup ads, or opens new web browser windows at random intervals. Users generally reject adware because:

- Adware may display objectionable content, such as gambling sites or pornography.
- Frequent popup ads can interfere with a user's productivity.
- Popup ads can slow a computer or even cause crashes and the loss of data.
- Unwanted advertisements can be a nuisance.

Some adware goes beyond affecting the user's computer experience. For example, a user who visits online automobile sites to view specific types of cars can be tracked by adware and classified as someone interested in buying a new car. Based on the sequence and type of websites visited, the adware can also determine whether the surfers' behavior suggests they are close to making a purchase or are also looking at competitors' cars. This information is gathered by adware and then sold to automobile advertisers, who send the users regular mail advertisements about their cars or even call the user on the telephone.

Ransomware One of the fastest-growing types of malware is ransomware. **Ransomware** prevents a user's device from properly operating until a fee is paid. One type of ransomware locks up a user's computer and then displays a message that purports to come from a law enforcement agency. This message, using official-looking imagery, states that the user has performed an illegal action such as downloading pornography and must immediately pay a fine online by entering a credit card number. The computer remains "held hostage" and locked until the ransom payment is made by entering a numeric credit card number (the ransomware does not lock the numeric keys on the keyboard). Figure 3-5 shows a ransomware message from the Symantec website in its Security Response Center.

Figure 3-5 Ransomware message

Source: Symantec Security Response

The ransom demanded is seldom exorbitant, and usually a payment of $300–$500 is required. The reason for the relatively modest fee is that attackers have determined the ideal price point. The ransom is not set so high that a user cannot or will not pay it or be motivated to contact law enforcement agencies. Instead, the lower ransom is usually seen by the user as more of a "nuisance fee" that is within the ability of most users to pay.

Another variation displays a fictitious warning that there is a problem with the computer such as (in a touch of irony) a malware infection or imminent hard drive failure. No matter what the condition of the computer, the ransomware always reports that there is a problem. This ransomware variation tells users that they must immediately purchase additional software online to fix the problem that in fact does not exist. The warning appears to be legitimate because it mimics the appearance of genuine software and—unlawfully—uses legitimate trademarks or icons. The ransomware example in Figure 3-6 uses color schemes and icons similar to those found on legitimate Windows software. Users who provide their credit card number to make the purchase find that the attackers simply capture that information and then use the card number for their own purposes.

In most instances, the ransomware embeds itself into the computer so that the message cannot be closed and rebooting the computer has no effect. In addition, most ransomware is part of a "package" in which other malware is also installed on the computer. This makes it very difficult to completely disinfect an infected computer.

Figure 3-6 Ransomware computer infection

Source: Microsoft Security Intelligence Report

Delete Data The payload of other types of malware deletes data on the computer. This may involve deleting important user data files, such as documents or photos, or erasing vital operating system files so that the computer will no longer properly function.

One type of malware that is frequently used to delete data is a logic bomb. A **logic bomb** is computer code that is typically added to a legitimate program but lies dormant until it is triggered by a specific logical event. Once it is triggered, the program then deletes data or performs other malicious activities.

There have been several high-profile incidents in businesses regarding logic bombs. In one example, a Maryland government employee tried to destroy the contents of more than 4,000 servers by planting a logic bomb script that was scheduled to activate 90 days after his employment was terminated.[4] In another incident a temporary contract employee inserted a logic bomb that would delete data stored on computers regarding the project on which he was working after his contract expired; his plan was to have the company hire him back as a consultant—at a large fee—in order to fix the problem.[5] Logic bombs are difficult to detect before they are triggered. This is because logic bombs are often embedded in very large computer programs, some containing tens of thousands of lines of code, and a trusted employee can easily insert a few lines of computer code into a long program without anyone detecting it. In addition, these programs are not routinely scanned for malicious content.

Logic bombs have sometimes been used by legitimate software companies to ensure payment for their software. If a payment is not made by the due date, the logic bomb activates and prevents the software from being used again. In some instances, logic bombs even erase the software and the accompanying payroll or customer files from the computer.

For home computers most often a logic bomb is based on a specific time or date. When the computer system's internal clock reaches that time or date then the bomb detonates.

Logic bombs should not be confused with an *Easter egg*, which refers to an undocumented, yet benign hidden feature that launches by entering a set of special commands, key combinations, or mouse clicks. In an earlier version of Microsoft Excel there was actually an entire game called "The Hall of Tortured Souls" that was embedded as an Easter egg. Recent versions of the Google Chrome web browser running on Android devices also have an embedded game.

Modify System Security The payload of some types of malware attempts to modify the system's security settings so that more insidious attacks can be made. One type of malware in this category is called a backdoor. A **backdoor** gives access to a computer, program, or service that circumvents any normal security protections. Backdoors that are installed on a computer allow the attacker to return at a later time and bypass security settings.

Creating a legitimate backdoor is common practice by developers, who may need to access a program or device on a regular basis, yet do not want to be hindered by continual requests for passwords or other security approvals. The intent is for the backdoor to be removed once the application is finalized. However, in some instances backdoors have been left installed, and attackers have used them to bypass security.

Launch Attacks One of the common payloads of malware today is software that will allow the infected computer to be placed under the remote control of an attacker. This infected robot (*bot*) computer is known as a **zombie**. When hundreds, thousands, or even hundreds of thousands of zombie computers are gathered into a logical computer network, they create a **botnet** under the control of the attacker (**bot herder**).

Due to the multitasking capabilities of modern computers, a computer can act as a zombie while at the same time carrying out the tasks of its regular user. The user is completely unaware that his or her computer is being used for malicious activities.

Infected zombie computers wait for instructions through a *command and control* (C&C or C2) structure from the bot herders regarding which computers to attack and how.

A common botnet C&C mechanism used today is the Hypertext Transport Protocol (HTTP), which is the standard protocol for Internet usage, thus making it difficult to detect and block. For example, a zombie can receive its instructions by automatically signing in to a website that the bot herder operates or to a third-party website on which information has been placed that the zombie knows how to interpret as commands (this latter technique has an advantage in that the bot herder does not need to have an affiliation with that website). Other botnets use blogs or send specially coded attack commands through posts on the Twitter social networking service or notes posted in Facebook.

Some bot herders use a "dead drop" C&C mechanism. First a bogus Google Gmail email account is set up and the zombie malware has the account username and password coded into it. The bot herder then creates a draft email message in Gmail but never sends it. At set times the zombie logs in to Gmail and reads the draft to receive its instructions. The benefits of this dead drop are that the email message is never sent so there is no record of it and all Gmail transmissions are protected so that they cannot be viewed by outsiders.

Table 3-3 lists some of the attacks that can be generated through botnets.

Type of attack	Description
Spamming	Botnets are widely recognized as the primary source of spam email. A botnet consisting of thousands of zombies enables an attacker to send massive amounts of spam.
Spreading malware	Botnets can be used to spread malware and create new zombies and botnets. Zombies have the ability to download and execute a file sent by the attacker.
Manipulating online polls	Because each zombie has a unique Internet Protocol (IP) address, each "vote" by a zombie will have the same credibility as a vote cast by a real person. Online games can be manipulated in a similar way.
Denying services	Botnets can flood a web server with thousands of requests and overwhelm it to the point that it cannot respond to legitimate requests.

Table 3-3 Uses of botnets

In many ways a botnet is the ideal base of operations for attackers. Zombies are designed to operate in the background, often without any visible evidence of their existence. By keeping a low profile, botnets are sometimes able to remain active and operational for years.

The ubiquitous always-on Internet service provided by residential broadband ensures that a large percentage of zombies in a botnet are accessible at any given time. This has resulted in a staggering number of botnets. One botnet may have contained more than 50 million zombies, and another botnet was responsible for sending 60 percent of all worldwide spam (or over 60 billion emails daily).[6]

Security in Your World

Dr. Antonelli had just finished describing to Sanne the different types of attacks that a computer faces today. "I had no idea there were that many!" she said. "OK, so what do I do now? If antivirus software can't stop everything, do I need an anti-something for each one?"

Dr. Antonelli set down his coffee cup. "No, not really. There are some different protections that you'll want to install on your computer. But there are two things that I would consider to be critically important. The first is to make sure your new computer will automatically install software patches." Sanne pulled out a piece of paper from her backpack. "I remember that we talked about patches last week. These are software updates that fix software security problems on your computer." Dr. Antonelli smiled. "Yes, that's right. You will want your computer to automatically install them, so you don't have to do anything."

"That sounds good," said Sanne. "Now what's the second thing?" Dr. Antonelli said, "The second thing is something that everybody knows that they should do, but still very few people do it as regularly as they should. It's one of the most important protections you have against these attackers. Can you guess what it is?" Sanne thought for a moment and said, "I'm afraid you've got me stumped. What is it?" Dr. Antonelli opened up a desk drawer and pulled out a portable hard drive. "It's backing up everything on your computer on a device like this," he said. "With all the new attacks that come out each day, the overwhelming odds are that your new computer could get infected. Having a good backup will protect you so you won't lose anything that's on your computer."

Sanne smiled. "That's what I need. How do we get started?"

Computer Defenses

Because of the large number and different types of attacks and the fact that new attacks are being continually introduced, there are several security protections that a computer should have installed and configured to resist attacks. The defenses include managing patches, configuring personal firewalls, installing antimalware software, monitoring User Account Control, creating data backups, and knowing how to recover from an attack.

Managing Patches

Early operating systems were simply program loaders whose job was to launch applications. As more features and graphical user interfaces (GUIs) were added, they became more complex. Due to the increased complexity of operating systems, unintentional

vulnerabilities were introduced that could be exploited by attackers. In addition, new attack tools made what were once considered secure functions and services on operating systems now vulnerable.

Microsoft's first operating system, MS-DOS v1.0, had 4,000 lines of code, while Windows 10 is estimated to have up to 80 million lines.

To address the vulnerabilities in operating systems that are uncovered after the software has been released, software vendors usually deploy a software "fix." A fix can come in a variety of formats. A security **patch** is a publicly released software security update intended to repair a vulnerability. **Feature updates** are enhancements to the software to provide new or expanded functionality, but do not address a security vulnerability. A **service pack** is software that is a cumulative package of all patches and feature updates.

Microsoft releases what it calls "service bulletins" that typically contain a set of patches for a group of software products, such as all the supported versions of Windows. These bulletins include a severity rating system that rates the impact of the vulnerability that the patch is fixing (Critical, Important, Moderate, or Low) and an Exploitability Index, which is the likelihood of an attack based on the vulnerability. This Exploitability Index is "1: Consistent Exploit Code Likely" (an attack could consistently exploit the vulnerability), "2: Inconsistent Exploit Code Likely" (an attack could be created but it would not function consistently in each case), and "3: Functioning Exploit Code Unlikely" (attacks based on the vulnerability are unlikely to be released).

Modern operating systems have the ability to perform automatic patch updates to their software so that the user's computer interacts with the vendor's online update service to receive the patches. Prior to Windows 10, Microsoft users had several options regarding accepting or even rejecting patches. These options included *Install updates automatically*, *Download updates but let me choose whether to install them*, *Check for updates but let me choose whether to download and install them*, and *Never check for updates*. However, with the release of Windows 10 Microsoft significantly changed its security update procedures and user options. These changes include:

- *Forced updates*. Users cannot refuse or delay security updates. All updates will be downloaded and installed automatically. Windows 10 Home edition users will also automatically receive feature updates, although Windows 10 Professional edition users can postpone feature updates for several months.
- *No selective updates*. Unlike in previous versions of Windows, users cannot select individual Windows updates to download and install. However, users can select if they wish to receive updates for other installed Microsoft products (such as Office).
- *Continual updates*. Microsoft traditionally has released its patches on the second Tuesday of each month, called "Patch Tuesday," unless the patch addresses a particularly serious vulnerability, and it is then released immediately. However, with Windows 10

Microsoft has said that patches will be distributed whenever they become available and are needed.

- *Choose when to reboot*. Some updates require that the computer must be rebooted in order for the updates to take effect. Now users can choose either the default "Automatic" (in which the computer will reboot whenever the computer is not being used) or "Notify to schedule restart" (the computer will not automatically reboot but the user will first be notified to schedule a reboot).
- *More efficient distribution*. If there are multiple Windows 10 devices connected to a network, then each device does not have to download the updates over the Internet individually. Instead, once one device has downloaded the updates these can then be distributed to the other devices across the local network. In addition, Windows will not download updates on mobile devices unless that device is connected to an unrestricted Wi-Fi network (so that it does not use the cellular data connections that users pay for).
- *Up-to-date resets*. With previous versions of Microsoft Windows, if a computer needed to be reset to its original configuration then all of the subsequent patches had to be reinstalled, a process that often would take hours of time and require the user to be at the computer in order to manage multiple reboots. With Windows 10, a "PC Reset" will install the current up-to-date Windows software.

The patch update options for Microsoft Windows 10 are seen in Figure 3-7.

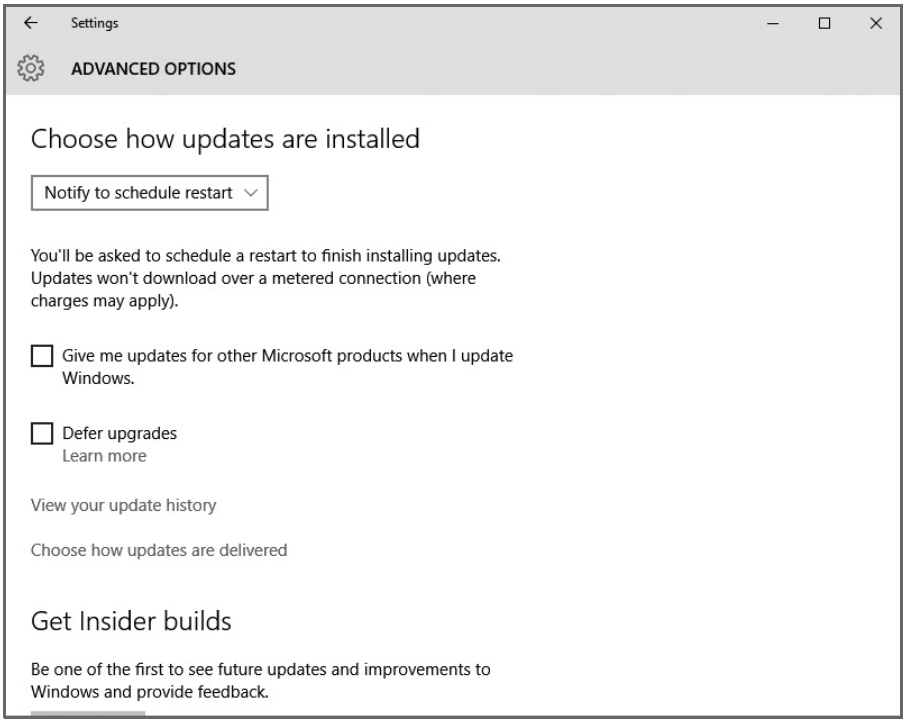


Figure 3-7 Windows 10 update options

Microsoft is following the trend among software vendors to automatically download and install patches without any user intervention or options. The Google Chrome web browser is automatically updated whenever it is necessary without even telling the user—and there are no user configuration settings to opt out of the updates.

Examining Firewalls

Both national and local building codes require commercial buildings, apartments, and other similar structures to have a *firewall*. In building construction, a firewall is usually a brick, concrete, or masonry unit positioned vertically through all stories of the building. Its purpose is to contain a fire and prevent it from spreading.

A computer **firewall**, technically called a *packet filter*, serves a similar purpose: it is designed to limit the spread of malware. There are two types of firewalls. A software-based **personal firewall** runs as a program on the local computer to block or filter traffic coming into and out of the computer. All modern operating systems include a *host-based application firewall*. As the name suggests these firewalls are *application-based*. That is, an application or program running on a computer may need to communicate with another computer on the local network or an Internet server to send and receive information. These transmissions normally would be blocked by the firewall. With an application firewall, an opening in the firewall just for that program can be created by the user simply approving the application to transmit (called *unblocking*). This is more secure than permanently opening an entry point on the firewall itself: when a permanent firewall opening is made it always remains opened and is then susceptible to attackers, but when an opening is unblocked by an application firewall it is opened only when the application needs it. The settings for the Windows personal firewall are shown in Figure 3-8.

Figure 3-8 Windows personal firewall settings

Application firewalls can limit the spread of malware into the computer as well as prevent a user's infected computer from attacking other computers. For most application firewalls, inbound connections (data coming in from another source) are blocked unless there is a specific firewall rule setting that allows them in. Outbound connections (data going out to another source) are allowed unless there is a rule that blocks them and the outbound rules are turned on.

The second type of firewall is a hardware-based **network firewall**. Although a personal host-based application software firewall that runs as a program on one computer is different in many respects from a network firewall designed to protected an entire network, their functions are essentially the same: to inspect network traffic and either accept or deny entry. Table 3-4 compares these two types of firewalls. Hardware firewalls are usually located at the "edge" of the network as the first line of defense defending the network and devices connected to it. Most home users have a network firewall as part of their networking equipment that provides Wi-Fi access or connects computers and devices such as printers together.

Even home networking devices that do not have a specific firewall can still perform functions that limit entry into the network by unauthorized outsiders.

Function	Personal firewall	Network firewall
Location	Runs on a single computer	Located on edge of the network
Scope of protection	Protects only computer on which it is installed	Protects all devices connected to the network
Type	Software that runs on computer	Separate hardware device
Filtering	Based on programs running on the computer	Provides sophisticated range of filtering mechanisms

Table 3-4 **Personal and network firewalls**

Personal and hardware firewalls overlap in some ways, but each provides unique benefits. A hardware firewall is isolated from the computer so that an infection on the computer that could compromise the personal firewall will not impact the hardware firewall. However, a hardware firewall knows very little about what program on the computer is making an outgoing connection. For this reason you should have both a personal and hardware firewall.

Users should periodically examine both their personal firewalls and network firewalls. These checks should include determining that the firewalls are functioning (many types of malware attempt to turn off firewalls), performing an external test on the firewall, and making sure that unnecessary entry points have not been made through the firewall.

The steps for examining a Windows 10 personal firewall are covered in Hands-On Project 2-1.

Installing Antimalware Software

At one time installing antimalware software was considered to be the primary defense against attackers. One of the first antimalware software security applications was **antivirus** (**AV**) software. This software can examine a computer for any infections as well as monitor computer activity and scan new documents that might contain a virus (this scanning is typically performed when files are opened, created, or closed). If a virus is detected, options generally include cleaning the file of the virus, quarantining the infected file, or deleting the file. Figure 3-9 shows the settings of a typical AV program.

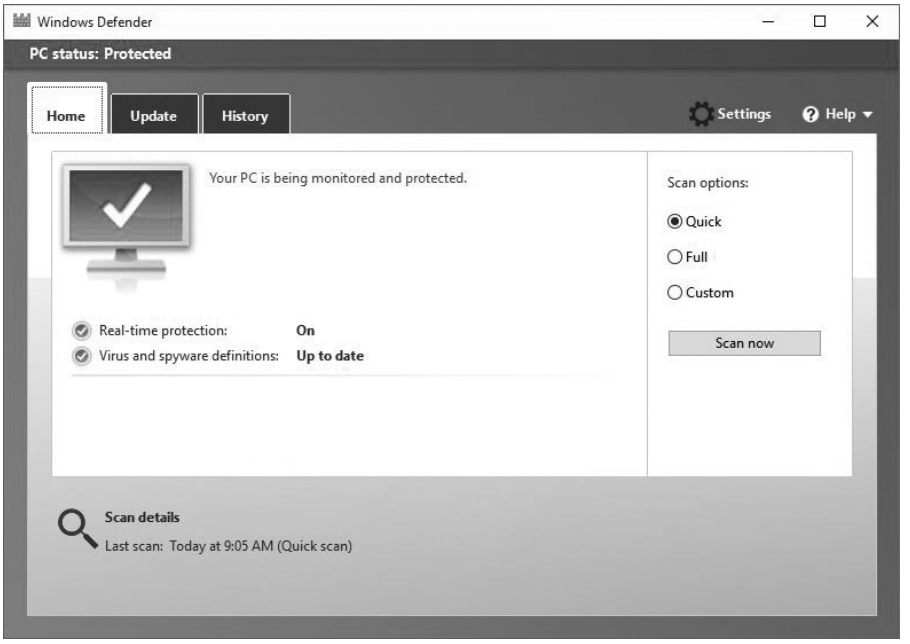


Figure 3-9 AV program settings

However, today AV is considered only part of a protection plan. Viruses are only one type of attack: worms, Trojans, spyware, ransomware, and many other types of malware all require different protections. And even if AV could offer comprehensive protection, AV vendors cannot keep up with the sheer number of new attacks. This is because many AV products scan files by attempting to match known virus patterns against potentially infected files, called *static analysis*. The host AV software contains a virus scanning engine and a database of known virus signatures, which are created by extracting a sequence of characters—a string—found in the virus that then serves as a virus's unique "signature." This database is called the **signature file**. By

comparing the virus signatures against a potentially infected file (called *string scanning*), a match may indicate an infected file. The weakness of static analysis is that the AV vendor must constantly be searching for new viruses, extracting virus signatures, and distributing those updated databases to all users. Any out-of-date signature file could result in an infection.

A recent study examined how long it took the four major AV vendors to distribute their updates to protect against the latest viruses. After looking at "tens of thousands" of instances of malware and the average time it took the AV vendors to distribute their updates, the study found that after one week the AV software still was not able to detect 28 percent of the malware, and it took almost six months for the AV software to protect against all of the malware.[7]

This is not to say that AV software is completely unnecessary. A newer approach to AV is *dynamic heuristic detection*, which uses a variety of techniques to spot the characteristics of a virus instead of attempting to make matches using a signature file. One technique used is *code emulation* in which a "virtual" environment is created that simulates the central processing unit (CPU) and memory of the computer. Any questionable program code is executed in the virtual environment (no actual virus code is executed by the real computer) to determine if it is a virus. Dynamic heuristic detection helps improve the capabilities of AV software.

The difference between static analysis and dynamic heuristic detection is similar to how airport security personnel in some nations screen for terrorists. A known terrorist attempting to go through security can be identified by comparing his face against photographs of known terrorists (static analysis). But what about a new terrorist for whom there is no photograph? Security personnel can look at the person's characteristics—holding a one-way ticket, not checking any luggage, showing extreme nervousness—as possible indicators that the individual may need to be questioned (dynamic heuristic detection).

Another type of antimalware software is **antispyware** that helps prevent computers from becoming infected by different types of spyware. One example of antispyware is a **popup blocker**, which is a separate program or a feature incorporated within a browser that stops popup advertisements from appearing. A browser popup blocker allows the user to limit or block most popups. Users can select the level of blocking, ranging from blocking all popups to allowing specific popups. When a popup is detected, an alert can be displayed in the browser such as: *Popup blocked; to see this popup or additional options click here.*

Despite that fact that antimalware software like AV provides only limited protection it is nevertheless recommended that users install AV software to take advantage of the protection that it does provide. However, antimalware software should be considered as only one tool in a large arsenal of weapons that must be employed to defend against attackers.

Monitoring User Account Control (UAC)

A *user account* indicates the privilege level of a user; that is, it tells the computer which files and folders can be accessed and what configuration changes can be made to the computer.

Microsoft Windows users can be assigned one of three different types of user accounts, each giving a different level of control over the computer:

- *Guest accounts*. Guest accounts are intended for users who need temporary use of a computer. There are very few settings that can be changed from a guest account.
- *Standard accounts*. A standard account is designed for everyday computing activities and allows some settings to be modified.
- *Administrator accounts*. The highest level of user account is an administrator account. This provides the most control over a computer.

Modern operating systems contain a function that alerts the user to an event that the operating system is about to perform and may also ask explicit permission from the user to perform this task. This helps prevent a Trojan or other malware from secretly making changes or installing new software. In Microsoft Windows this security function is called **User Account Control (UAC)**. UAC provides information to users and obtains their approval before a program can make a change to the computer's settings.

When requesting approval from the user the UAC can perform two actions. First, it can temporarily switch to *secure desktop mode* in which the entire screen is dimmed. Desktop mode prevents an attacker from manipulating any UAC messages that appear on the screen. Second, a UAC dialog box appears. If the user has an administrator account, the user must click *Continue* or *Yes* before UAC will allow any changes to be made or software installed. Figure 3-10 shows UAC settings. If the user's level is Standard or Guest, then the administrator password must be entered by another person before any changes are permitted.

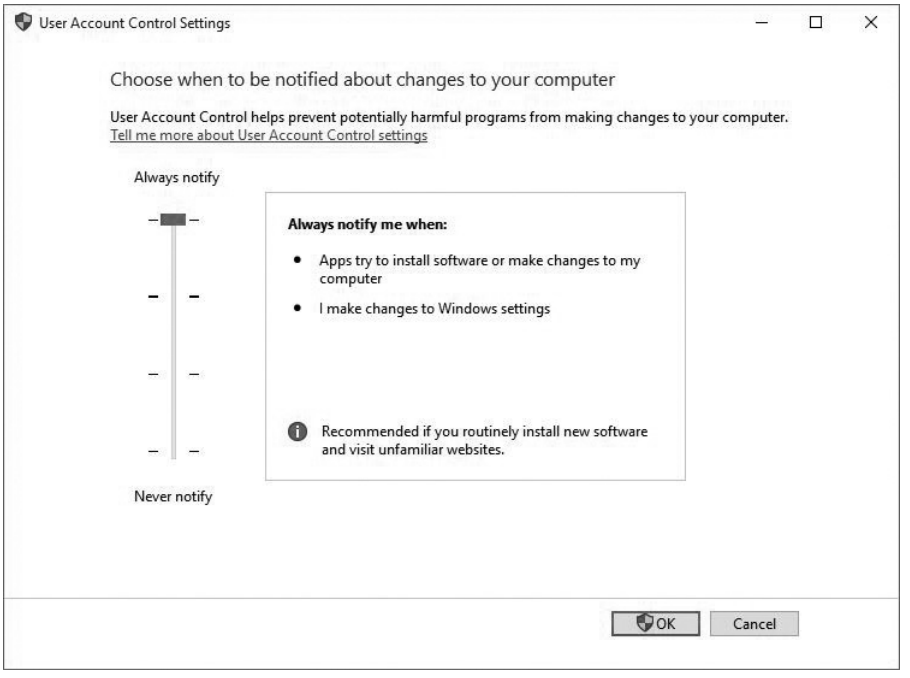


Figure 3-10 User Account Control settings

The Windows UAC interface also provides extended information. A shield icon warns users if they attempt to access any feature that requires UAC permission. In addition, the UAC prompt includes a description of the requested action. The UAC prompts are color-coded to indicate the level of risk, from red (highest risk) to yellow (lowest risk).

There are four levels of UAC that can be adjusted to the user's preference. These are *Always notify*, *Notify me only when programs try to make changes to my computer*, *Notify me only when programs try to make changes to my computer (do not dim my desktop)*, and *Never notify*. It is recommended that the highest protection level of *Always notify* should be set.

You should always pause when a UAC dialog box appears instead of just giving immediate approval. What were you doing when the box appeared? For example, if you were starting a software installation, then the UAC warning reflects your actions and you may approve it. However, if you were visiting a website or performing a software download and the UAC box appears, then you should deny the request.

Creating Data Backups

One of the most important defenses against attacks is frequently overlooked: it is to regularly create **data backups**. Creating a data backup means copying files from a computer's hard drive onto other digital media that is stored in a secure location. Data backups protect against computer attacks because they can restore infected computers to their properly functioning state. Data backups can also protect against hardware malfunctions, user error, software corruption, and natural disasters.

There are several ways to easily create backups. These may be divided into scheduled backups and continuous backups.

Scheduled Backups A *scheduled backup* is performed intentionally by the user. It could be performed every morning at 3:00 (automated) or whenever the user remembers that a backup is needed (on demand). When performing scheduled backups several questions must be asked in advance to ensure the backup meets the users' needs.

The first question is *what* data should be backed up. All user-created files that cannot be easily or quickly recreated should be backed up. These include any personal files, such as documents created with a word processor, digital photos, personal financial data, and other similar information. However, should programs installed on the computer, such as the operating system or a word processor program, also be backed up? If these programs are readily available elsewhere or can be retrieved easily, such as from a DVD or downloaded online, there is little need to back them up along with the data files.

The main reason to back up programs along with user data files is that it allows an infected computer to be completely restored more quickly from the backup instead of installing all of the programs individually from DVDs or online before restoring the user data files.

The second question is *what media* should be used. Optical disc storage like a DVD, although compact and inexpensive, nevertheless requires the user to be present during the backup process to continually "feed" discs into the drive if multiple discs are required. A more viable option is to use a portable external hard drive. These devices connect to the USB port of a computer and provide backup capabilities; they are fast, portable, and can store large amounts of data.

The third question is *where to store* the backup. Consider a user who installs a second hard drive in his computer to back up the data from primary hard drive each night. This would allow for the primary hard drive to be restored quickly in the event of an infection or primary hard drive failure. However, what about a theft, fire, tornado, or lightning strike? These events could destroy both the primary hard drive and the backup hard drive. It is recommended that a copy of the data backup be stored at an off-site location, such as at a work location, a friend's house, or on the Internet.

Home users should consider using the 3-2-1 backup plan. This plan says that you should always maintain *three* different copies of your backups (that does not count the original data itself) by using at least *two* different types of media on which to store these backups (a separate hard drive, an external hard drive, a USB device, online storage, etc.) and store *one* of the backups offsite.

The final question is *how frequently* the backup should be performed. It is recommended that backups be performed once per day on computers that are being used frequently. If that is not possible then a regular schedule (such as every Tuesday and Friday) should be implemented.

Modern operating systems can perform automated backups, and third-party software is also available that provides additional functionality.

Continuous Backups A *continuous backup* is one that is performed continually without any intervention by the user. Software monitors what files have changed and automatically updates the backed up files with the most recent versions. The first continuous backups were performed locally: changes to files on a user's hard drive were automatically updated to an attached USB hard drive. Today continuous backups can be performed online. There are several Internet services available that provide features similar to these:

- *Automatic continuous backup*. Once the initial backup is completed, any new or modified files are also backed up. Usually the backup software will "sleep" while the computer is being used and perform backups only when there is no user activity. This helps to lessen any impact on the computer's performance or Internet speed.
- *Universal access*. Files backed up through online services can be made available to another computer.

- *Optional program file backup*. In addition to user data files these services can as an option also back up all program and operating system files.
- *Delayed deletion*. Files that are copied to the online server will remain accessible for up to 30 days before they are deleted. This allows a user to have a longer window of opportunity to restore a deleted file.
- *Online or disc-based restore*. If a file or the entire computer must be restored this can be done online. Some services also provide the option of shipping to the user the backup files on DVDs.

The advantage of online continuous backups is they are performed automatically and stored at a remote location. These may provide the highest degree of protection today to users.

There are several services, some of which are free, that automatically back up any files that are placed in a designated folder on your computer. Although not as full-featured as online backup services, they do allow for backups of important data files.

Recovering from Attacks

Just as a homeowner cannot be absolutely certain that her house will never be broken into even if she has installed strong door locks, the same is true with computer security.

Preparation is the key to recovering from an attack. For Microsoft Windows users it is important to create a *recovery drive* (that can run from a USB flash drive) or *system repair disc* (that runs from a DVD disc) that can help repair Windows in the event of a serious error, such as errors caused by malware. In addition, there are several software vendors online that offer free downloadable *rescue discs*. These are downloadable images that can be used to create a bootable DVD or USB flash drive. When the computer is restarted it will bypass the infected hard drive and boot from the DVD or flash drive, which will then automatically scan and disinfect the computer.

Exceptional Security

MANAGING PATCHES—If necessary, set your computer's operating system to always install the most recent security patches automatically. Monitor the downloads and if the computer must be rebooted, select "Restart Now" as soon as the patches are installed; do not wait until later or select a restart time for a later date because the patches do not take effect until the computer is rebooted. Permit updates for other software products to also be installed. Pay attention to current security news and watch for information about patches that are available for other software, such as

(continues)

Adobe Flash and Oracle Java. Download and install these patches immediately. Switch to software products that perform automatic patch downloads and installations, such as Google Chrome.

MONITOR FIREWALLS—Periodically check the settings of the host-based application firewall to monitor which applications have permission to go through the firewall. Consider deleting those applications that are rarely used but still have permission to go through the firewall. Although all application firewalls have outbound rules they are not always turned on by default, essentially defeating their purpose. Be sure that outbound rules are turned on. Check the firewall on your wireless router or similar network device and be sure that it is turned on. Disable Universal Plug and Play (UPnP) on network firewalls. If you must absolutely use UPnP, look for a router that offers detailed status information about the state of forwarded ports, such as the app that made the UPnP request and details on the currently active port forwarding rules.

DATA BACKUPS—Implement a strong backup strategy. Have an image of your computer's hard drive automatically backed up every day. Every few days copy this image to an external USB hard drive that is stored in another room. Once per week copy the image to another external USB hard drive and keep this drive stored at a remote location. Periodically test a backup by installing it on another computer. Or consider an online continuous backup service.

OTHER—Set UAC to "Always notify." Make it a habit to pause when the UAC prompt appears and think about what you are doing before approving the request. Install AV software and run a complete scan at least once per week. Create a recovery disk of your operating system and store it at a remote location. Identify websites that have software that can be downloaded to boot and scan a computer for malware. Download the software and use it to scan your computer to check it for malware and to become familiar with the process. Save the name of the website with your recovery disk (do not save the scanning software since it can become quickly out of date).

Chapter Summary

- Malware is malicious software that enters a computer system without the owner's knowledge or consent and includes a wide variety of damaging actions. One method of classifying the various types of malware is by using the primary trait that the malware possesses. These traits are circulation, infection, concealment, and payload capabilities.
- One of the types of malware that has the primary trait of circulation is a computer virus. A virus is malicious computer code that reproduces itself on the same computer. A virus inserts itself into a computer file (a data file or program) and then tries to reproduce on the same computer as well as unload its malicious payload. Another type of such malware is a worm, which travels through a network and is designed to take advantage of a vulnerability in an application or an operating system in order to enter a user's computer. Once the worm has exploited the vulnerability on one system, it immediately searches for another computer that has the same vulnerability. A Trojan is

a program advertised as performing one activity but in addition does something malicious. Some malware has as its primary trait avoiding detection. A rootkit is a set of software tools used to hide the actions or presence of other types of software.

- The destructive power of malware is to be found in its payload capabilities. When the payload allows an attacker to execute virtually any command on the victim's computer, this is called arbitrary code execution. Most often arbitrary code execution takes advantage of a vulnerability in the operating system software or an application program. Different types of malware are designed to collect important data from the user's computer and make it available to the attacker. Spyware is a general term used to describe software that secretly spies on users by collecting information without their consent. One type of spyware is a keylogger, which silently captures and stores each keystroke that a user types on the computer's keyboard. Adware is a software program that delivers advertising content in a manner that is unexpected and unwanted by the user. Ransomware locks up a user's computer and then displays a message that purports to come from a law enforcement agency or security software company and demands payment of a fine online before the computer is released.
- The payload of other types of malware deletes data on the computer. A logic bomb is computer code that is typically added to a legitimate program but lies dormant until it is triggered by a specific logical event. The payload of some types of malware attempts to modify the system's security settings so that more insidious attacks can be made. One type of malware in this category is called a backdoor. A backdoor gives access to a computer, program, or service that circumvents any normal security protections. One of the most common payloads of malware today is software that will allow the infected computer to be placed under the remote control of an attacker. This infected computer is known as a zombie. When zombie computers are gathered into a logical computer network, they create a botnet.
- Due to the increased complexity of software, unintentional vulnerabilities were introduced that could be exploited by attackers. In addition, new attack tools made what were once considered secure functions and services on operating systems now vulnerable. A security patch is a publicly released software security update intended to repair a vulnerability. Modern operating systems have the ability to perform automatic patch updates so that the user's computer interacts with the vendor's online update service to receive the patches.
- A computer firewall is designed to limit the spread of malware. There are two types of firewalls. A software-based personal firewall runs as a program on the local computer to block or filter traffic coming into and out of the computer. A hardware-based network firewall is usually located at the "edge" of the network as the first line of defense defending the network and devices connected to it.
- One of the first antimalware software security applications was antivirus (AV) software that can examine a computer for any infections as well as monitor computer activity and scan new documents that might contain a virus. Many AV products scan files by attempting to match known virus patterns against potentially infected files. The host AV software contains a virus scanning engine and a database of known virus signatures called the signature file. Due to delays in updating signature files AV software is no longer considered as the premier means of providing protection.

Another type of antimalware software is antispyware. One example of antispyware is a popup blocker, which is a separate program or a feature incorporated within a browser that stops popup advertisements from appearing.

- Modern operating systems contain a function that alerts the user to an event that the operating system is about to perform and may also ask explicit permission from the user to perform this task. In Microsoft Windows this security function is called User Account Control (UAC).
- One of the most important defenses against attacks is to create data backups on a regular basis. Creating a data backup means copying files from a computer's hard drive onto other digital media that is stored in a secure location. Data backups protect against computer attacks because they can restore infected computers to their properly functioning state. A scheduled backup is one that is performed intentionally by the user, whereas a continuous backup is one that is performed continually without any intervention by the user.
- In spite of the best defenses, sooner or later an attack on a computer may be successful. System repair discs can be created from the operating system to help repair the software in the event of a successful attack. In addition, there are several software vendors online that offer free downloadable rescue discs.

Key Terms

Definitions for key terms can be found in the Glossary for this text.

adware	firewall	rootkit
antispyware	keylogger	service pack
antivirus (AV)	logic bomb	signature file
arbitrary code execution	malware	spyware
backdoor	network firewall	Trojan horse (Trojan)
bot herder	patch	User Account Control (UAC)
botnet	personal firewall	worm
computer virus (virus)	popup blocker	zombie
data backup	ransomware	
feature update	remote code execution	

Review Questions

1. A(n) _____ requires a user to transport it from one computer to another.
   a. adware
   b. worm
   c. rootkit
   d. virus

2. Which of these is NOT an action that a virus can take?
   a. transport itself through the network to another device
   b. reformat the hard disk drive
   c. cause a computer to crash
   d. erase files from a hard drive
3. Which malware locks up a user's computer and then displays a message that purports to come from a law enforcement agency?
   a. virus
   b. ransomware
   c. worm
   d. Trojan
4. Which of the following is not a type of malware that has as its primary trait circulation and/or infection?
   a. Trojan
   b. virus
   c. worm
   d. botnet
5. A user who installs a program that prints out coupons but in the background silently collects her passwords has installed a _____.
   a. virus
   b. worm
   c. Trojan
   d. logic bomb
6. Malware payload allows an attacker to execute virtually any command on the victim's computer; this is called _____.
   a. arbitrary code execution
   b. remote configuration
   c. master control
   d. extension reach code
7. Which of these could NOT be defined as a logic bomb?
   a. Erase all data if John Smith's name is removed from the list of employees.
   b. Reformat the hard drive three months after Susan Jones left the company.
   c. Send spam email to all users in the company.
   d. If the company's stock price drops below $10, then credit Jeff Brown with 10 additional years of retirement credit.

8. What is access a computer, program, or service that circumvents any normal security protections called?
   a. hole
   b. backdoor
   c. trapdoor
   d. honey pit
9. Which of these is a general term used for describing software that gathers information without the user's consent?
   a. pullware
   b. adware
   c. spyware
   d. scrapeware
10. Which statement regarding a keylogger is NOT true?
   a. Software keyloggers are easy to detect.
   b. Keyloggers can be used to capture passwords, credit card numbers, or personal information.
   c. Hardware keyloggers are installed between the keyboard connector and computer keyboard USB port.
   d. Software keyloggers can be designed to send captured information automatically back to the attacker through the Internet.
11. Botnets are composed of _____.
   a. Internet Relay Chat (IRC) instruments
   b. zombies
   c. herders
   d. spam
12. Each of the following is the reason why adware is scorned, except _____.
   a. it displays the attackers programming skills
   b. it can interfere with a user's productivity
   c. it displays objectionable content
   d. it can cause a computer to crash or slow down
13. Each of the following is a typical feature of a fee-based Internet backup service except _____.
   a. backup to an external hard drive
   b. universal access
   c. file feedback information
   d. delayed deletion

14. How many carriers must a virus have to replicate and attack?
    a. one
    b. two
    c. three
    d. four

15. Which level of UAC provides the lowest level of security?
    a. Universal notify
    b. Always notify
    c. Never notify
    d. Notify on demand
16. Which of the following enhancements to software provides new or expanded functionality but does not address security vulnerabilities?
    a. feature update
    b. patch
    c. service pack
    d. resource package
17. Which type of firewall is an external hardware device?
    a. personal firewall
    b. remote firewall
    c. network firewall
    d. application resource firewall
18. The database that contains the sequence of characters of a virus is called the _____.
    a. string file
    b. malware DB
    c. virus resource file
    d. signature file
19. Each of the following is a question that the user should ask regarding data backups except _____.
    a. What content should be backed up?
    b. Who should do the backup?
    c. Where should the backup be stored?
    d. How frequently should be backup be performed?

20. A _____ is a downloadable image that can be used to scan a computer for malware.
    a. system repair disc
    b. rescue disc
    c. resource disc
    d. clean disc

Hands-On Projects

Project 3-1: Configure Microsoft Windows Security

It is important that security settings be properly configured on a computer in order to protect it. In this project, you will examine several security settings on a Microsoft Windows 10 computer.

This project shows how to configure Windows security for a personal computer. If this computer is part of a computer lab or office, these settings should not be changed without the proper permissions.

1. Click **Start** and **Settings**.
2. Click **Update and security**.
3. If necessary click **Windows Update** in the left pane.
4. Click **Advanced options,** then under **Choose how updates are installed** change to **Automatic (recommended)**.

Remember that the safest approach is to restart the device as soon as any updates have been installed.

5. Click **Give me updates for other Microsoft products when I update Windows.** This will allow for updates for Microsoft software such as Office to also be updated.
6. Click **View your update history** to see the updates that have been installed on your computer.
7. Click the **back arrow**.
8. Click the **back arrow** to return to **Update & Security**.
9. Click **Windows Defender**. This is the Microsoft AV product that is part of Windows 10.
10. Be sure that all the settings are set to On.
11. Click **Use Windows Defender**. The Windows Defender dialog box appears.
12. Under **Scan options**: be sure that **Quick** is selected.

13. Now perform a Quick scan of the most essential files. Click **Scan now**. Depending upon your system it may take several minutes to complete. What was the result of the scan?
14. Click the **History** tab. Be sure that **Quarantined items** is selected and click **View details**. Has Defender already identified suspicious files on this computer and placed them in quarantine? When you are finished, close Windows Defender.
15. In the **Find a setting** search box enter **UAC** and press **Enter**.
16. Click **Change User Account Control Settings**. The **User Account Control Settings** dialog box opens.
17. Move the slider through all of the choices and notice the description of each.
18. Position the slider to **Always notify**. Why is this the best security setting? Click **OK** and then **Yes**.
19. Now check your personal firewall. Return to the **Settings** window. Click **Network and Internet**.
20. Click **Ethernet**.
21. Click **Windows Firewall** to view the firewall settings.
22. Click **Allow an app or feature through Windows Firewall** to display the **Allowed apps** dialog box as seen in Figure 3-11. Scroll through the list of apps that can transmit through the firewall. Are there apps that you are not using that should be removed from this list?

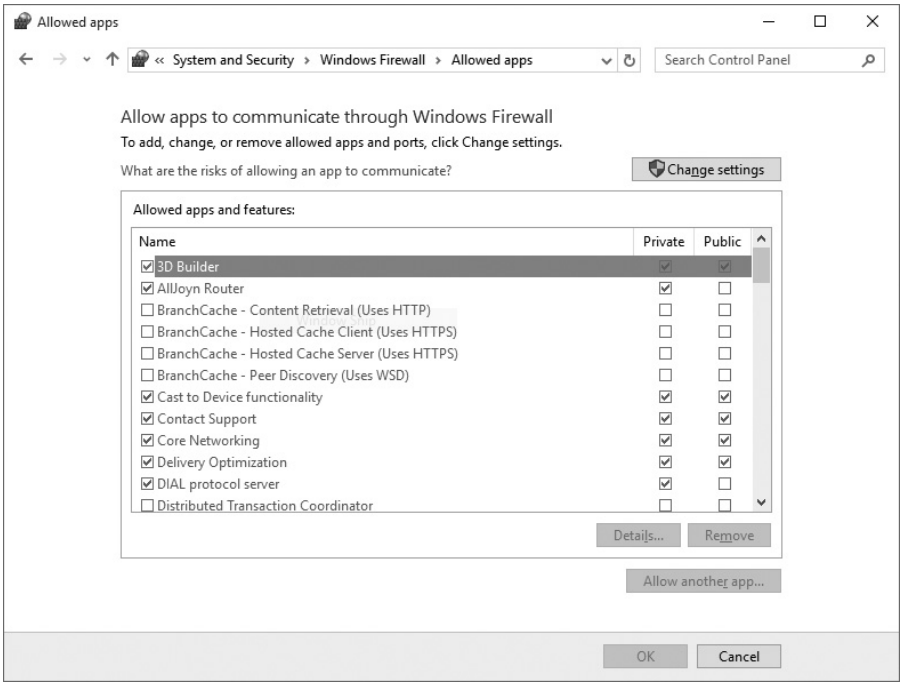


Figure 3-11 Allowed apps dialog box

23. Close the **Allowed apps** dialog box.
24. Close the **Settings** dialog box.
25. Finally, create a recovery drive for this computer. First insert a blank USB flash drive.
26. In the Windows search box enter **recoverydrive.exe** and press **Enter**. Click **Yes** in the UAC.
27. The Recovery Drive dialog box appears. Click **Next**.
28. The system gathers the appropriate files. In the **Select the USB flash drive** dialog box select the appropriate drive. Click **Next**.
29. Click **Create** to complete the process.
30. After the drive has been created close all windows.

Project 3-2: Test Antivirus Software

What happens when antivirus software detects a virus? In this project you download a virus test file to determine how your AV software reacts. The file downloaded is not a virus but is designed to appear to an antivirus scanner as if it were a virus.

You need to have antivirus software installed and running on your computer to perform this project.

1. Open your web browser and enter the URL **www.eicar.org/86-0-Intended-use.html** (if you are no longer able to access the site through the web address, use a search engine to search for "Eicar anti-malware test file").
2. Read the "INTENDED USE" information. The file you will download is not a virus but is designed to appear to an antivirus scanner as if it were a virus.
3. Click **DOWNLOAD**.
4. Click the file **eicar.com**, which contains a fake virus. A dialog box may open that asks if you want to download the file. Wait to see what happens. What does your antivirus software do? Close your antivirus message and if necessary click **Cancel** to stop the download procedure.
5. Now click **eicar_com.zip**. This file contains a fake virus inside a compressed (ZIP) file. What happened? Close your antivirus message and, if necessary, click **Cancel** to stop the download procedure.

If your antivirus software did not prevent you from accessing the eicar_com.zip file, when the File Download dialog box appears, click **Save** and download the file to your desktop or another location designated by your instructor. When the download is complete, navigate to the folder that contains the file and right-click it. Then, click **Scan for viruses** on the shortcut menu (your menu command might be slightly different). What happened after the scan?

6. Click **eicarcom2.zip**. This file has a double-compressed ZIP file with a fake virus. What happened? Close your antivirus message and, if necessary, click **Cancel** to stop the download procedure.
7. If necessary erase any files that were saved to your computer.
8. Close all windows.

Project 3-3: Analyze Files and URLs for Viruses Using VirusTotal

VirusTotal, a subsidiary of Google, is a free online service that analyzes files and URLs in order to identify potential malware. VirusTotal scans and detects any type of binary content, including a Windows executable program, Android, PDFs, and images. VirusTotal is designed to provide a "second opinion" on a file or URL that may have been flagged as suspicious by other AV software. In this project, you will use VirusTotal to scan a file and a URL.

1. Use Microsoft Word to create a document that contains the above paragraph about VirusTotal. Save the document as **VirusTotal.docx**.
2. Now save this document as a PDF. Click **File** and **Save As**.
3. Under **Save as type:** select **PDF (*.pdf)**.
4. Save this file as **YourName-VirusTotal.pdf**.
5. Exit Word.
6. Open your web browser and enter the URL **www.virustotal.com** (if you are no longer able to access the site through the web address, use a search engine to search for "Virus Total").
7. If necessary click the **File** tab.
8. Click **Choose File**.
9. Navigate to the location of **YourName-VirusTotal.pdf** and click **Open**.
10. Click **Scan it!**
11. If the **File already analysed** dialog box opens, click **Reanalyse**.
12. Wait until the analysis is completed.
13. Scroll through the list of AV vendors that have been polled regarding this file. A green checkmark means no malware was detected.
14. Click the **File detail** tab and read through the analysis.
15. Use your browser's back button to return to the VirusTotal home page.
16. Click **URL**.
17. Enter the URL of your school, place of employment, or other site with which you are familiar.

18. Click **Scan it!** If the **URL already analysed** dialog box opens, click **Reanalyse**.
19. Wait until the analysis is completed.
20. Scroll through the list of vendor analysis. Do any of these sites indicate **Unrate site** or **Malware site**?
21. Click **Additional information**.
22. How could VirusTotal be useful to users? How could it be useful to security researchers? However, could it also be used by attackers to test their own malware before distributing it to ensure that it does not trigger an AV alert? What should be the protections against this?
23. Close all windows.

Project 3-4: Creating a Disk Image Backup

To back up programs and operating system files in addition to user files, one solution is to create a disk image. A disk image file is created by performing a complete sector-by-sector copy of the hard drive instead of backing up using the drive's file system. In this project, you download Macrium Reflect to create an image backup.

1. Use your web browser to go to **www.macrium.com**.
2. Under **Download Trial** click **Home**.
3. Click **DOWNLOAD**.
4. Save the file to the desired location and then launch the program.
5. In the Macrium Reflect Download Agent click **Trial software**
6. Click **Download**.
7. Install this program onto your computer by accepting the default settings.
8. Launch Macrium Reflect.
9. If you are asked **Do you want to create Rescue Media Now?** Click **No**.
10. In the left pane click **Create an image of the partition(s) required to backup and restore Windows**.
11. The **Disk Image** dialog box appears. Select the location to store the backup. You cannot store the backup on the same hard drive that you are creating the image on; you must store it on another hard drive in that computer or on an external USB hard drive. Under **Destination** select the appropriate location. Click **Next**.
12. Do not edit the plan for the backup. Click **Next**.
13. Click **Finish**.
14. If necessary, click **Run this backup now** and then click **OK** to begin the backup. Note that, depending on the size of the data to be backed up and the speed of the computer, it will take several minutes to perform the backup.
15. Close all windows.

Case Projects

Case Project 3-1: Online Backup Services

There are several good continuous online backup services that can help make data backup easy for the user. Use a search engine to search for *online backup service reviews*, and select three different services. Research these services and note their features. Create a table that lists each service and compare their features. Be sure to also include costs. Which would you recommend? Why?

Case Project 3-2: Information Security Community Site Activity

The Information Security Community Site is an online companion to this textbook. It contains a wide variety of tools, information, discussion boards, and other features to assist learners. Go to *community.cengage.com/infosec*. Sign in with the login name and password that you created in Chapter 1.

What should be the penalty for those who create viruses, worms, and other destructive malware? Prison time? Monetary fines? How should it be enforced? And would this deter attackers? Record your responses on the Community Site discussion board.

Additional Case Projects for this chapter are available through the MindTap online learning environment.

References

1. "FireEye Advanced Threat Report–2H 2012," *FireEye*, Apr. 3, 2013, accessed Jan. 3, 2014, www2.fireeye.com/rs/fireye/images/fireeye-advanced-threat-report-2h2012.pdf.
2. "The First Computer Virus," accessed Mar. 3, 2011, www.worldhistorysite.com/virus.html.
3. "Anti-Spyware Coalition Definitions Document," *Anti-Spyware Coalition*, Nov. 19, 2007, accessed Aug. 13, 2015, www.antispywarecoalition.org/documents/definitions.htm.
4. Cluley, Graham, "Fannie Mae Worker Accused of Planting Malware Timebomb," *Naked Security Sophos Blog*, accessed Mar. 3, 2011, http://nakedsecurity.sophos.com/2009/01/29/fannie-mae-worker-accused-planting-malware-timebomb/.
5. DaBoss, "Logic Bombs," *Computer Knowledge*, Mar. 1, 2013, accessed Aug. 13, 2015, http://www.cknow.com/cms/vtutor/logic-bombs.html.

6. Thomas, Karl, "Nine bad botnets and the damage they did," *We Live Security*, Feb. 25, 2015, accessed Aug. 13, 2015, http://www.welivesecurity.com/2015/02/25/nine-bad-botnets-damage/.
7. "2015: Time to fix broken malware strategies," *Damballa Day before Zero Blog*, Feb. 12, 2015, accessed Aug. 24, 2015, https://www.damballa.com/time-to-fix-malware-strategies/.

chapter 4

Internet Security

After completing this chapter you should be able to do the following:

- Explain how the Internet and email function
- Describe how attackers can use browser vulnerabilities, malvertising, and drive-by downloads to spread malware
- List the security risks associated with using email
- Describe how to use web browser settings and browser additions to create stronger security
- List several Internet security best practices

Security in Your World

"Finished!" said Magdalena as she saved her document. Magdalena, Aaron, and Nubia attended a local college and also worked together at an assisted living facility. During their dinner hour they tried to catch up on their class assignments in the break room.

Nubia frowned and said, "You mean you're finished already? It seems like you just started." Magdalena turned off her wireless mouse. "That assignment wasn't hard. It was for my *Current Trends in Technology* class. We just had to explain the top three steps that we would take to protect ourselves while we were surfing online." "OK," said Nubia, "What did you say?" "I said the most important thing to do was to visit only known websites. I mean, if you're shopping online you should only visit sites of major retailers and not little mom-and-pop sites. That will keep you safe," she said.

Aaron set down his glass. "I'm not sure that's right," he said. Magdalena looked puzzled and asked, "But why not?" Aaron leaned forward and picked up his backpack. "Do you remember when my computer got infected last semester? The person at our school's IT Tech Support who fixed it told me that my computer was infected because I had visited *Walmart.com*. Everybody who visited it got infected just like I did."

Nubia opened his computer. "I remember you telling us about it. Didn't Marty's computer get infected that way, too?" Aaron nodded his head. "Yes, I think so. Here, I still have the article that Tech Support gave me." Aaron fished around in his backpack and pulled out some papers. "It says that big-name sites are actually more likely to get infected than smaller sites. That's because more people visit the big sites and it gives the attackers the chance to infect more computers." Nubia looked at Magdalena and said, "And isn't the Internet all about visiting new sites? If I only went to big-name sites that I had heard of before then I wouldn't go to very many places."

Aaron set down the papers. "I've got a question. Can you look at a website—either a big-name site or a small one—and somehow tell if it's safe or not?" Magdalena, Nubia, and Aaron all quietly sat in their chairs. "I don't know," Nubia finally said. "How can you tell if a website is safe?"

The impact of the Internet on our world has been nothing short of astonishing. Although today's Internet has its roots all the way back in the late 1960s, it was only used by researchers and the military for almost a quarter of a century. With the introduction of web browser software in the early 1990s, along with the spread of telecommunication connections at work and home, the Internet became useable and accessible to almost everyone. This created a

seismic shift across society. First, a virtually limitless amount of information was suddenly available at users' fingertips. Second, not only did it give unprecedented access to information, but the Internet also created a collective force of tremendous proportions. For the first time in human history, mass participation and cooperation across space and time is possible, empowering individuals and groups all over the world. The Internet is truly having a revolutionary impact on how we live.

But for all of the benefits that the Internet has provided, it also has become the primary pathway for attackers to reach our computers and personal information. When we connect a computer to the Internet to receive valuable information, we also are exposing that computer to malicious attacks. An unprotected computer that is connected to the Internet can be infected in a matter of minutes, and the number of Internet-based attacks continues to increase dramatically each day.

In this chapter, you will learn about some of the attacks on computers that come through the Internet and what can be done to minimize those risks. First, you'll see how the Internet works and then you'll identify the types of risks with using it. After that, you'll examine the defenses that can be set up to make using this valuable tool a more enjoyable and productive experience.

How the Internet Works

The **Internet** is a global network that allows devices connected to it to exchange information. Yet there are two common misconceptions regarding the Internet. First, the Internet is not made up of individual devices (desktop computers, tablets, laptops, smartphones, etc.) but instead is composed of networks around the world to which devices are attached. The Internet is often called an international *network of computer networks*. Second, it is not owned or controlled by any single organization or government entity. Instead, these networks are operated by industry, governments, schools, and even individuals, who all loosely cooperate to make the Internet a global information resource.

Understanding how some of the basic Internet tools work helps to provide the foundation for establishing Internet security. The two main Internet tools that are used today are the World Wide Web and email. It is through these tools that the overwhelming majority of Internet attacks occur.

The World Wide Web

The **World Wide Web** (**WWW**), better known as the *web*, is composed of Internet server computers on networks that provide online information in a specific format. The format is based on the **Hypertext Markup Language** (**HTML**). Web authors use HTML to combine text, graphic images, audio, video, and *hyperlinks* (which allow users to jump from one area on the web to another with a click of the mouse button) into a single document. Instructions written in HTML code specify how a local computer's web **browser** (a program for showing webpages) should display the words, pictures, and other elements on a user's screen, as shown in Figure 4-1.

Figure 4-1 Browser displaying HTML code

Web servers distribute HTML documents based on a set of standards, or *protocols*, known as the **Hypertext Transfer Protocol (HTTP)**. HTTP is a subset of a larger set of standards for Internet transmission known as the **Transmission Control Protocol/Internet Protocol (TCP/IP)**.

The word *protocol* comes from two Greek words for *first* and *glue*, and originally referred to the first sheet glued onto a manuscript on which the table of contents was written. The term later evolved to mean an "official account of a diplomatic document" and was used in France to refer to a formula of diplomatic etiquette.

Figure 4-2 illustrates how a webpage is displayed based on a user's request. The web browser on the user's computer sends a request to a remote web server. The web server knows by information given that the request is for an HTML document and responds by sending the entire HTML document (again using HTTP), which is then stored on the user's local computer. Finally the user's web browser then displays the document.

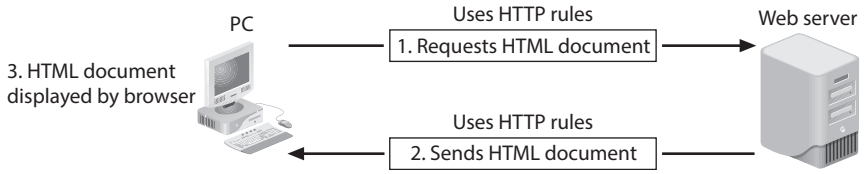


Figure 4-2 Web transmission process

In the web transmission process the local computer does not view the HTML document on the web server; rather, the entire document is transferred and then stored on the local computer before the browser displays it. This transfer-and-store process creates opportunities for sending different types of malicious code to the user's computer, and makes web browsing a potentially risky security experience.

Email

Since developer Ray Tomlinson sent the first email message in 1971, email has become an essential part of everyday life. It is estimated that over 2.3 million emails are sent every second, increasing at a rate of 5 percent each year. By 2019 it is estimated that there will be 246 billion emails sent daily by over 2.9 billion email users.[1]

There are two different electronic email systems that are in use today. An earlier email system uses two TCP/IP protocols to send and receive messages: the **Simple Mail Transfer Protocol** (**SMTP**) handles outgoing mail, while the **Post Office Protocol** (**POP**, more commonly known as *POP3* for the current version) is responsible for incoming mail. POP3 is a basic protocol that allows users to retrieve messages sent to an email server by using a local program running on their computer called an *email client*. The email client connects to the POP3 server and downloads the messages onto the local computer. After the messages are downloaded, they may be erased from the POP3 server.

Internet Mail Access Protocol (**IMAP**) is a more recent and advanced electronic email system. With IMAP, the email remains on the email server and is not downloaded to the user's computer. Mail can be organized into folders on the mail server and read from any device: desktop computer, tablet, smartphone, and so on. IMAP users can even work with email while offline. This is accomplished by downloading email onto the local computer without erasing the email on the IMAP server. A user can read and reply to email offline. The next time a connection is established, the new messages are sent and any new email is downloaded. The current version of IMAP is IMAP4.

Older email clients typically used only POP3. Using a web browser to view email messages on an email server, like Google Gmail, generally use IMAP. Most mobile devices are also configured to use IMAP.

Email **attachments** are documents that are attached to an email message, such as word processing documents, spreadsheets, or pictures. These attachments are encoded in a special format and sent as a single transmission along with the email message itself.

When the receiving computer receives the attachment, it converts it back to its original format.

Internet Security Risks

There are several risks that users face from using the Internet. These include browser vulnerabilities, malvertising, drive-by downloads, cookies, and email risks.

Browser Vulnerabilities

In the early days of the web, users viewed *static* content (information that does not change) such as text and pictures through a web browser. As the Internet increased in popularity, the demand rose for *dynamic* content that can change, such as animated images or customized information. However, basic HTML code could not provide these functions.

The solution came in several different forms. One solution was to allow scripting code to be downloaded from the web server into the user's web browser. Another solution took the form of different types of additions that could be added to a web browser to support dynamic content. These web browser additions are extensions, plug-ins, and add-ons.

Scripting Code One means of adding dynamic content is for the web server to download a "script" or series of instructions in the form of computer code that commands the browser to perform specific actions. **JavaScript** is the most popular scripting code. Because JavaScript cannot create separate "stand-alone" applications, the JavaScript instructions are embedded inside HTML documents. When a website that uses JavaScript is accessed, the HTML document that contains the JavaScript code is downloaded onto the user's computer. The user's web browser then executes that code. Figure 4-3 illustrates how JavaScript works.

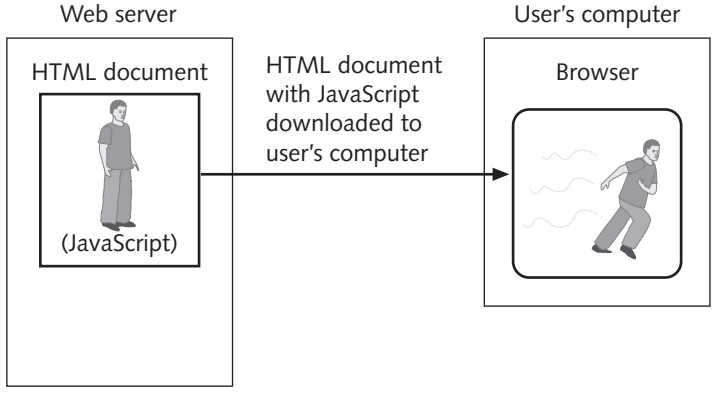


Figure 4-3 JavaScript

Visiting a website that automatically downloads code to run on a local computer can obviously be dangerous: an attacker could write a malicious script and have it downloaded and executed on the user's computer. There are different defense mechanisms intended to prevent JavaScript programs from causing serious harm. These defenses are listed in Table 4-1.

Defense	Explanation
Limit capabilities	JavaScript does not support certain capabilities. For example, JavaScript running on a local computer cannot read, write, create, delete, or list the files on that computer.
Sandboxing	By only permitting JavaScript to run in a restricted environment ("sandbox") this can limit what computer resources it can access or actions it can take.
Same origin	This defense restricts a JavaScript downloaded from Site A from accessing data that came from Site B.

Table 4-1 JavaScript defenses

However, there are still security concerns with JavaScript. A malicious JavaScript program could capture and remotely transmit user information without the user's knowledge or authorization. For example, an attacker could capture and send the user's email address to a remote source or even send a fraudulent email from the user's email account. Other JavaScript attacks can be even more malicious. An attacker's JavaScript program could scan the user's network and then send specific commands to disable security settings, or redirect a user's browser to an attacker's malicious website.

Extensions

Extensions expand the normal capabilities of a web browser for a specific webpage. Most extensions are written in JavaScript so that the browser can support dynamic actions. Because extensions act as part of the browser itself, they generally have wider access privileges than JavaScript running in a webpage. Extensions are browser-dependent, so that an extension that works in the Google Chrome web browser will not function in the Microsoft Edge browser.

Plug-Ins

A **plug-in** adds new functionality to the web browser so that users can play music, view videos, or display special graphical images within the browser that normally it could not play or display. Technically a plug-in is a *third-party binary library* that lives outside of the "space" that a browser uses on the computer for processing and serves as the link to external programs that are independent of the browser. A single plug-in can be used on different web browsers, such as Google Chrome, Mozilla Firefox, and Microsoft Internet Explorer.

One common plug-in supports Java. Unlike JavaScript, **Java** is a complete programming language that can be used to create stand-alone applications. Whereas JavaScript is embedded in an HTML document, Java can also be used to create a separate program called a *Java applet*. Java applets are stored on the web server and then downloaded onto the user's computer along with the HTML code, as shown in Figure 4-4. Java applets can perform interactive animations, mathematical calculations, or other simple

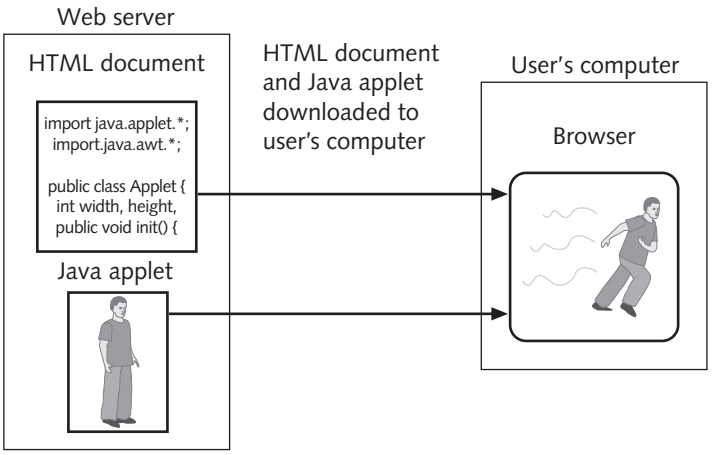


Figure 4-4 Java applet

tasks very quickly because the user's request does not have to be sent to the web server for processing and then returned; instead, all of the processing is done on the local computer by the Java applet.

The most widely used plug-ins for web browsers are Java, Adobe Flash player, Apple QuickTime, and Adobe Acrobat Reader. However, there are tens of thousands of freely available plug-ins, created by not only well-known organizations but also by individual coders.

One popular blogging tool for users to post their personal blogs supports 39,848 plug-ins.[2]

Add-Ons Another category of tools that add functionality to the web browser are called **add-ons**. Add-ons add a greater degree of functionality to the entire browser and not just to a single webpage as with a plug-in. In contrast to plug-ins, add-ons can do the following:

- Create additional web browser toolbars
- Change browser menus
- Be aware of other tabs open in the same browser process
- Process the content of every webpage that is loaded

Table 4-2 compares browser extensions, plug-ins, and add-ons.

Name	Description	Location	Browser support	Examples
Extension	Written in JavaScript and has wider access to privileges	Part of web browser	Only works with a specific browser	Download selective links on webpage, display specific fonts
Plug-in	Links to external programs	Outside of web browser	Compatible with many different browsers	Audio, video, PDF file display
Add-on	Adds functionality to browser itself	Part of web browser	Only works with a specific browser	Dictionary and language packs

Table 4-2 Browser additions

It is easy to see how extensions, plug-ins, and add-ons can be security risks. Because of the large number of these browser tools available, created by a large number of programmers, they often have serious security vulnerabilities. Attackers have targeted vulnerable plug-ins as a means to insert malware into a user's computer or in some instances take over complete control of the computer.

Adobe Flash is one of the most popular plug-ins that attackers target. In one five-year span over 324 vulnerabilities in Flash were exploited by attackers.[3]

Due to the risks associated with extensions, plug-ins, and add-ons efforts are being made to minimize them. Some web browsers now block plug-ins like Adobe Flash, while other browsers use a "Click to Play" feature that enables a plug-in only after the user gives approval. In addition, the most recent version of HTML known as **HTML5** standardizes sound and video formats so that plug-ins like Flash are no longer needed. Yet with the large number of these browser tools still available they will likely continue to remain a target of attackers.

Malvertising

When visiting a typical website it is common for advertisements to be displayed around the pages. For example, visiting a fitness-tracking website will often result in ads promoting athletic shoes, sports drinks, weight loss, and other related products being displayed. These ads do not usually come from the main site itself; instead, most mainstream and high-trafficked websites outsource the ad content on their pages to different third-party advertising networks. When a user goes to the site's page, the user's web browser silently connects to dozens of advertising network sites from which ad banners, pop-up ads, video files, and pictures are sent to the user's computer.

Attackers have turned to using these third-party advertising networks to distribute their malware to unsuspecting users who are visiting a well-known website. Attackers may infect the third-party advertising networks so that their malware is distributed through ads sent to users' web browsers. Or the attackers may promote themselves as reputable third-party advertisers while in reality they are distributing their malware through the ads. This is known as **malvertising** (*malicious advertising*) or a *poisoned ad attack* and is illustrated in Figure 4-5. An ad that contains malware secretly redirects visitors who

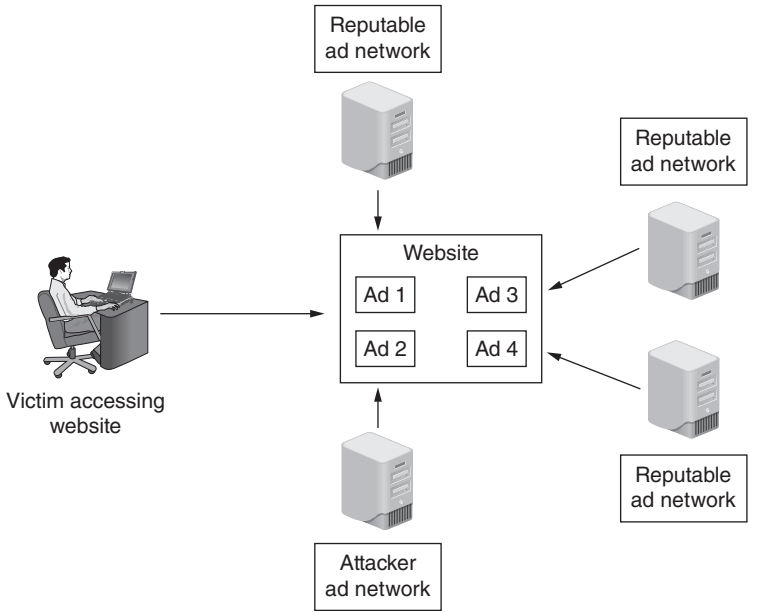


Figure 4-5 Malvertising

receive it to the attacker's webpage that then downloads Trojans, zombies, and ransomware onto the user's computer, often through vulnerabilities in extensions, plug-ins, and add-ons.

The New York Times, Reuters, Yahoo!, Bloomberg, and Google, among many others, have all been infected with malvertising. In one year, 12.4 billion "malvertisements" were distributed, an increase of over 300 percent from the previous year. The growth of malvertising is also credited with a 41-percent increase in ad-blocking software, now used by 198 million users.[4]

Malvertising has a number of advantages for the attacker:

- Malvertising occurs on "big-name" websites, such as news publications that attract many visitors each day who are keeping abreast of the latest news stories. These unsuspecting users, who otherwise would avoid or be suspicious of less popular sites, are deceived into thinking that because they are on a reputable site they are free from attacks.
- Usually the website owners have no knowledge of malware being distributed through their website through ads. This is because they do not know what type of ad content a third-party ad network is displaying on their site at any given time.
- Ad networks rotate content very quickly, so that not all visitors to a site are infected, making it difficult to determine if malvertising was actually the culprit of an attack. And even when an ad is pinpointed in an investigation as malicious, it is virtually impossible to prove which ad network was responsible.

- Because advertising networks configure ads to appear according to the user's computer (which browser or operating system they are using) or identifying attributes (their country locations or search keywords they used to find the site) attackers can narrowly target their victims. For example, an attacker who wants to target U.S. federal government employees might distribute ads with malicious content for anyone who entered "Government travel allowance" into a search engine.

Because these attacks can precisely target their victims, often "high value victims" are pinpointed. For example, an attacker might place malicious ads before individuals who are conducting a keyword-search for hotel rates at an upcoming security conference.

Preventing malvertising is a difficult task. Website operators are unaware of the types of ads that are being displayed, users have a false sense of security going to a "mainstream" website, and turning off ads that support plug-ins such as Adobe Flash often disrupts the user's web experience.

Because Adobe Flash is used in 84 percent of ad banners and because the Flash plug-in is seen as a weak security link, malvertisers frequently create Flash-based advertising malware.[5]

Drive-By Downloads

Whereas malvertising seeks to infect a mainstream website through third-party advertising networks, other attacks attempt to infect the website directly. In some instances this can result in a user's computer becoming infected just from viewing the website. Such occurrences are called **drive-by downloads**.

Attackers first identify a well-known website and then attempt to inject malicious content by exploiting it through a vulnerability in the web server. These vulnerabilities often permit the attacker to gain direct access to the web server's underlying operating system and then inject new content into the compromised website. The injected content is virtually invisible to the naked eye.

Technically speaking, in drive-by downloads, the attackers use a *zero pixel IFrame*. IFrame (short for *inline frame*) is an HTML element that allows for one HTML document to be embedded inside the main document. It is almost impossible to see a zero pixel IFrame.

When unsuspecting users visit an infected website, their browsers download code, usually written in JavaScript, that targets a vulnerability in the user's browser. If the script can run successfully on the user's computer, it can instruct the browser to connect to the attacker's own web server to download malware, which is then automatically installed and executed on the user's computer.

Unlike a traditional download that asks for the user's permission to perform an action, a drive-by download can be initiated simply by visiting an infected website.

Cookies

HTML does not have a mechanism for a website to track whether a user has previously visited that site. Any information that was entered on a previous visit, such as site preferences or the contents of an electronic shopping cart, is not retained by HTML so that the web server can identify repeat customers. Instead of the web server asking the user for the same information each time the site is visited, the server can store user-specific information in a file on the user's local computer and then retrieve it for a future visit. This file is called a **cookie**.

A cookie can contain a variety of information based on the user's preferences when visiting a website. For example, if a user inquires about a rental car at the car agency's website, that site might create a cookie that contains the user's travel itinerary. In addition, it may record the pages visited on a site to help the site customize the view for any future visits. Cookies can also store any personally identifiable information (name, email address, work address, telephone number, and so on) that was provided when visiting the site.

There are several different types of cookies:

- *First-party cookie.* A **first-party cookie** is created from the website that a user is currently viewing. For example, when viewing the website *www.cengage.com*, the cookie *CENGAGE* could be created and saved on the user's hard drive. Whenever the user returns to this site, that cookie would be used by the site to view the user's preferences and better customize the browsing experience.
- *Third-party cookie.* Some websites attempt to place additional cookies on the user's computer. These cookies often come from third-party advertising networks that advertise on the site and want to record the user's preferences in order to tailor ads to that user. These cookies are called **third-party cookies**.
- *Locally shared objects.* A **locally shared object (LSO)** is also called a *Flash cookie*, named after Adobe Flash. These cookies are significantly different from regular cookies in that they can store data more complex than the simple text that is typically found in a regular cookie. By default, LSOs can store up to 100 KB of data from a website, about 25 times as much as a regular cookie.

LSOs cannot be deleted through the browser's normal configuration settings as regular cookies can be. Typically, they are saved in multiple locations on the hard drive and also can be used to reinstate regular cookies that a user has deleted or blocked. Adobe, after much criticism, ultimately released an online tool to delete LSOs.

Cookies can pose both security and privacy risks. First-party cookies can be stolen and used to impersonate the user, while third-party cookies can be used to track the browsing or buying habits of a user. When multiple websites are serviced by a single marketing organization, cookies can be used to track browsing habits on all the client's sites. These organizations can track browsing habits from page to page within all their client sites and know which pages are being viewed, how often they are viewed, and the computer address of the viewing computer. This information can be used to infer what items the user may be interested in, and to target advertising to the user.

Many websites use advertising and tracking features to watch what sites are visited in order to create a profile of user interests. When you visit a site, it may create a unique identification number (like BTC081208) that is associated with your browser (your true identity is not known). Such features allow, for example, different ads to be displayed to baseball fans who are visiting spring training sites as opposed to those who are checking out tomorrow night's symphony performance. Not only does this tracking result in tailored ads being displayed as you surf, but it also ensures that the same ads do not keep appearing over and over.

Email Risks

One of the more common means of distributing attacks is through email. Email risks include spam, malicious attachments, and embedded hyperlinks.

Spam The amount of **spam**, or unsolicited email, which goes through the Internet, can be measured in the hundreds of billions of messages sent *daily*. The reason why users receive so many spam messages that advertise drugs, cheap mortgage rates, and items for sale is because sending spam is a lucrative business. It costs spammers very little to send millions of spam email messages. Almost all spam is sent from botnets: a spammer who does not own a botnet can lease time from other attackers ($40 per hour) to use a botnet of up to 100,000 infected computers to launch a spam attack. Even if spammers receive only a very small percentage of responses, they still make a large profit. For example, if a spammer sent spam to 6 million users for a product with a sale price of $50 that cost only $5 to make, and if only 0.001 percent of the recipients responded and bought the product (a typical response rate), the spammer would make over $270,000 in profit.

Text-based spam messages that include words such as *Viagra* or *investments* can easily be trapped by **spam filters** that look for these words and block the email. Because of the increased use of these filters, spammers have turned to another approach for sending out their spam. Known as **image spam**, it uses graphical images of text in order to circumvent text-based filters. Image spam cannot be filtered based on the content of the message because it appears as an image instead of text. These spam messages often include nonsense text so that it appears the email message is legitimate (an email with no text can prompt the spam filter to block it). Figure 4-6 shows an example of image spam.

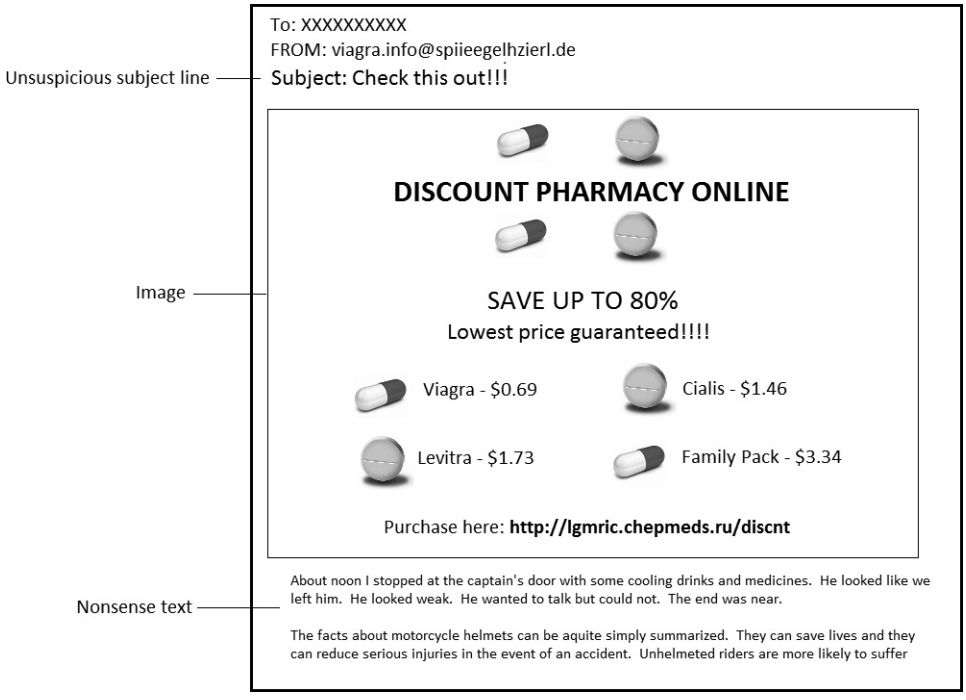


Figure 4-6 Image spam

Beyond just being annoying, spam significantly reduces work productivity as users spend time deleting spam messages. Spam is also costly to organizations that must install and monitor technology to block spam. However, one of the greatest risks of spam is that it is used to widely distribute malware.

Malicious Attachments Another common means of distributing attacks is through email attachments. Most users are unaware of the danger of attachments and routinely open any email attachment that they receive, even if it is from an unknown sender. Attackers often include in the subject line information that entices even reluctant users to open the attachment, such as a current event (*Check out this info about yesterday's hurricane*) or information about the recipient (*Is this really you in this picture?*).

Email-distributed malware will often take advantage of information contained on the user's computer. For example, malware can replicate by sending itself as an email attachment to all of the contacts in a user's email address book. The unsuspecting recipients, seeing that an email and attachment arrived from a "friend," typically with a provocative subject line, open the attachment and infect their computers.

Embedded Hyperlinks Many email messages have **embedded hyperlinks**, which are contained within the body of the message as a shortcut to a website. However, attackers can take advantage of embedded hyperlinks to direct users to the attacker's website

instead. This redirection can be easily accomplished because an embedded hyperlink can display only words and not the actual address of the website. For example, an attacker could create an embedded hyperlink that appears legitimate to the reader (*Click here to log in to Online Account Services*), yet the underlying web address to which the user is directed is the attacker's site. Even an embedded hyperlink that appears to be a legitimate web address (*www.onlineaccount.com*) can be crafted so that it goes to a different website (*www.attackers-dungeon.net*). The attacker's "look-alike" website asks the user to enter personal information, which the attacker captures and uses. In short, embedded hyperlinks can take users anywhere.

One organization distributed an email from the IT security department that specifically warned users not to click on embedded hyperlinks because of the danger associated with them. However, at the bottom of the email it said, "For more information click on this link"!

Security in Your World

"No more Internet for me!" said Magdalena. She had just finished looking at several websites about the security risks associated with using the Internet. "That will be the day!" laughed Aaron.

Nubia clicked on his mouse and said, "But aren't these attacks rare? I mean, I don't hear my friends talking about being attacked." Aaron smiled and said, "Well, I know you were in class the day we talked about this. Remember our instructor said that right now up to 25 percent of Internet users have infected computers, and most of them don't even know it? That's probably why your friends aren't telling you they've been attacked: they don't know that they have been!"

"So what do we do?" asked Magdalena. Aaron looked up from his computer and said, "This site I'm looking at seems to have a lot of good information about keeping yourself safe while on the Internet. This says there are some security settings and tools you can use to make surfing safer. But one of the most important things is to use common sense. Just like my mother used to tell me not to go to bed at night and leave my doors unlocked, there are some basic Internet security things you can do to protect yourself."

"I feel like I'm surfing the Internet with my doors unlocked!" Nubia laughed. "Here, let me see what it says."

Internet Defenses

Defending against Internet-based attacks begins with the foundation of first having the computer itself properly secured. This includes managing patches, configuring personal firewalls, installing anti-malware software, monitoring User Account Control, creating data backups, and knowing how to recover from an attack.

Basic computer security is covered in detail in Chapter 3.

Once the computer is properly secured, the additional defensive security steps to resist Internet-based attacks fall into three broad categories. These defenses include securing the web browser, maintaining email defenses, and following Internet security best practices.

Securing the Web Browser

One of the important lines of defense against Internet attacks is properly configuring the security settings on the web browser. It also involves installing additional browser security tools.

Web Browser Configuration Settings Modern web browsers are customizable and allow the user to tailor settings based on personal preferences. Beyond basic settings such as preferred home page and the size of displayed characters, browsers also allow the user to customize security and privacy settings.

Microsoft's Internet Explorer (IE) web browser includes over 60 configuration settings, many of which relate to security. One notable IE security feature is the ability to create web "zones," in which the user can set customized security for these zones and then assign specific websites to a zone. However, with the introduction of Windows 10, IE was replaced with a new browser called Edge, which lacks these features. Although IE is still part of Windows 10, Microsoft has stated that it is available only for compatibility and soon will no longer be supported.

Google's Chrome web browser is a browser that can be configured for security and offers a wide range of configuration settings, many of which relate to security and privacy. Figure 4-7 illustrates some of the Chrome security settings, several of which are described in the following list.

Figure 4-7 Google Chrome settings

Source: Google Chrome

Content Settings Google Chrome provides several Content Settings. These include:

- *Cookies*. Users can accept or deny either first-party or third-party cookies. Also cookies can be deleted once the browser is closed. In addition, exceptions can be made for specific websites, and all existing cookies can be viewed and selectively removed.
- *JavaScript*. Sites can be allowed to run JavaScript or blocked from running it, and exceptions can be made for specific websites.
- *Plug-ins*. Chrome is configured with several plug-ins that can run Adobe Flash and display PDF documents. Users can block all plug-ins or selective plug-ins. Another option prompts the user when a plug-in requests to run.
- *Pop-ups*. Users can block all pop-ups, permit all pop-ups, or selectively choose which sites to run pop-ups.
- *Unsandboxed plug-in access*. Some websites require plug-ins to have a direct "unsandboxed" access in order to run, such as streaming video or install additional software. Users can block all unsandboxed plug-ins, accept all unsandboxed plug-ins, or be prompted whenever a plug-in wants to run.

Google's Chrome web browser now automatically pauses Flash content that is not critical to a webpage, such as an advertisement. Critical webpage content, like a video, will continue to play without interruption. According to Google this improves battery life on mobile devices by as much as 15 percent.

Advanced Settings Google Chrome also has Advanced Settings that relate to security. These include:

- *Passwords and forms*. Users can be prompted whenever they enter a password for Chrome to save that password.
- *Downloads*. The default location of downloaded files can be set.
- *Clear browsing data*. All accumulated HTML files can be cleared from the computer's hard drive.
- *Use a web service to help resolve navigation errors*. Chrome can help prevent users who make a typing error when entering a Uniform Resource Locator (URL) address to being a victim of typo squatting and directed to an attacker's fake site.

Typo squatting is covered in Chapter 2.

- *Advanced sync settings*. Chrome can synchronize (sync) most of the user's settings and saved data including passwords across multiple computers and devices that have Chrome installed.

The Google sync setting also gives users the option of setting up a synchronizing passphrase which must be entered whenever a user signs in with his or her Google account password.

Browser Additions Almost all major web browsers support security-related browser additions, such as extensions, plug-ins, and add-ons. These may provide an additional level of security. Some of the more popular browser editions include:

- *Website reputation*. Extensions are available that help provide information about the trustworthiness of a website based on other users' experiences. Some extensions display a green (good), red (bad), or yellow (warning) along with an explanation of the site's rankings. However, website reputation extensions should be viewed as a caution but not an absolute reference as to the validity of a website.

The top-level domains that have the highest number of malicious sites are *.zip, .review, .country, .kim*, and *.cricket*. Almost 95 percent of the sites under these domains pose a potential threat to visitors.[6]

- *Plug-in validation*. A plug-in validation will examine the plug-ins that are being used and alert the user to any out-of-date or known vulnerable plug-ins.
- *URL expander*. Services are available that will "shrink" the size of a URL. For example, *www.cengage.com/search/productOverview.do?Ntt=ciampa|142326346114170521911849942311065619181&N=16&Ntk=APG%7CP_EPI&Ntx=mode+matchallpartial* could be reduced to *goo.gl/RbASFJ*. A URL expander extension allows the user to hover over a reduced URL in order to view its expanded format. This helps prevent attackers from disguising a URL that would take the user to an unsafe website.
- *Website tracker*. Extensions are available that allow the user to view the websites that track his or her activity. They also provide a means to quickly delete any cookies from unwanted tracking sites.
- *Ad blocker*. An ad blocker extension prevents any textual or video ads from appearing while a user is online.
- *Cookie stopper*. Some extensions can give the user the ability to decide if they want to accept or block any third-party cookies as sites attempt to create them on the user's computer.

Even though they provide a higher degree of security, these extensions should be used with a degree of caution, just as all extensions should.

Email Defenses

There are security defenses that can be configured to protect attacks through email. The most common are spam filtering, setting the security options in client-based email programs and web email, and securing attachments.

Spam Filters Beyond being annoying and disruptive, spam can also pose a serious security risk: spammers can distribute malware as attachments through their spam email messages. Spam filtering applications can be implemented on both the user's local computer as well as at the corporate or the Internet service provider level.

Most users actually receive only a small amount of spam in their local email inbox. The majority is blocked by the email service provider before it even reaches the user.

Email clients can be configured to filter spam that has bypassed a spam filter. The email client spam filtering settings often include these features to block spam:

- *Blocked senders*. A list of senders can be entered from whom the user does not want to receive any email, also known as a **blacklist**. Any message received from one of the senders is sent to the junk email folder. Several databases of blacklists are available on the Internet that include known spammers and others who distribute malicious content, and some sites allow users to download the lists and automatically add them to their email server.

- *Allowed senders*. A list of senders can be entered from whom the user will accept email, also known as a **whitelist**.
- *Blocked top-level domain list*. Email from entire countries or regions can also be blocked and treated as spam.

Microsoft Outlook automatically blocks over 80 different types of file attachments that may contain malware.

Email Security Settings In addition to spam filters on the local email client, there are other security settings that can be configured through the local email client and through using web email.

Local Email Client When using a local email client, these settings can improve security:

- *Read messages using a reading pane*. Most email clients contain a **reading pane**, which allows the user to read an email message without actually opening it. Received email messages can be viewed safely in the reading pane because malicious scripts and attachments are not activated or opened automatically in the reading pane.

Although malicious attachments might be blocked by using the email reading pane, messages and attachments from unknown or unsolicited senders should always be treated with caution.

- *Block external content*. Email clients can be configured to block external content in HTML email messages that are received, such as hyperlinks to pictures or sounds. When a user opens an email message or it is displayed in the reading pane, the computer downloads the external content so that the picture can be displayed or the sound played. In addition, spammers often send out spam to a wide range of email addresses, not knowing which email addresses exist or are accurate. In order to determine which email addresses are valid and actually exist, a spammer can note which email accounts downloaded the external content and then add those email accounts to their spam list. Blocking external content helps to prevent this.

Web Email When accessing webmail through a web browser, the following should be considered:

- *Set up account recovery options*. In the event that a password is forgotten or an account is locked out, having an account recovery option can provide the means for a password reset or information about the account sent to the user. Most web email allows users to set up either a recovery phone number or a different recovery email address. Having a recovery phone number allows a verification code to be sent as a text message so an account can be reentered. It also allows a notification alert to be sent in the event that an attacker is trying to break into the account.

- *Check account for unusual activity*. A good security practice is to periodically check the email account for any unusual activity. Were unfamiliar email messages sent from this account? Are there unusual deleted email messages in the Trash folder? Was the account accessed from a different location or at a different time than normal? If any of these occur the email password should be reset immediately.
- *Verify general settings*. The general email settings should also be regularly reviewed. Users should verify that any signature lines, accounts that receive forwarded email, contact list addresses, and other information is valid. If any suspicious information appears the email password should be reset immediately.

Attachments Because email attachments can contain malware, it is important to be wary regarding these types of files. With some email clients, when an attachment is received with an email message, the client will permit the user to preview the contents of the attachment without saving and opening it. This helps to protect the user from malicious code that may be embedded in the attachment because malicious scripts are disabled during attachment preview.

Attachment protection is also available in other applications. For example, Microsoft Office attachments (Word, Excel, PowerPoint, etc.) are automatically opened in **Protected View**, which is a read-only mode that disables editing functions. This helps prevent a malicious attachment from installing malware when it is opened by an unsuspecting user. A color-coded warning indicator at the top of the Office document explains why it was opened in Protected View. Users can click on the *Enable Editing* button in order to accept the file for editing.

As with all warnings, it is recommended that the Protected View *Enable Editing* button not be clicked without giving any thought to the source of the document. Protected View is designed to make the user pause and think about the risks before proceeding.

Internet Security Best Practices

There are several Internet security best practices when using email or surfing the web. These practices include:

- *Downloading files*. Download files only from well-established sites. Before downloading from any site, the user should check the domain and verify that he or she is on the actual site and not an imposter site. When prompted it is preferable to save a download to the hard drive instead of running it. This can give local security programs time to check the downloaded file before it is opened.
- *Controlling cookies*. Every browser has tools for controlling, blocking, and deleting cookies. However, completely blocking cookies may negatively impact what can be done on certain websites. If cookies cannot be blocked, the browser should be set to delete all cookies when the browser is closed.
- *Private browsing*. Most browsers have an option that allows the user to browse in "private." When in private browsing mode, information is not saved by the browser, such as pages that are visited will not be recorded to history or the address bar.

In addition, all cookies will be deleted at the end of the session, all temporary Internet files will be emptied at the end of the session, no forms, search bars, or text boxes through which data was entered will be saved, and downloads listed will be deleted (although the downloaded file itself will remain).

Private browsing does not provide anonymous surfing on the web; it only deletes data from the user's computer after the session has ended.

- *Browsing history*. Accessing a user's browsing history is a means for a website or another person to collect information about activity and preferences. For added privacy users should delete their browsing history.
- *Pop-up blockers*. Because pop-ups may contain malware the browser's pop-up blocker should be turned on.
- *Clearing the cache*. Web browsers store pages, images, and downloaded content to a temporary area (*cache*) when visiting websites. This allows the browser to speed up access to sites by loading pages from the cache rather than downloading content again when returning to a site. Over time a cache may consume a large amount of hard drive storage space and even cause the browser to slow down. The browser's cache should be cleared on a regular basis. It also can protect privacy since it deletes stored content and information.

Exceptional Security

USE LINUX—Because most malware is directed against Windows and Apple computer systems, use Linux to access critical online sites such as banking sites. Create a DVD disc with the MakuluLinux Aero, Elementary OS, Mint, or a similar Linux distribution. Restart the computer to load Linux from the disc and use its built-in browser. Because it is running only from a DVD, any downloaded malware cannot infect the computer.

LOCK DOWN THE BROWSER—Use a browser that automatically accepts all patches. Also use a browser that has Adobe Flash built-in so that it will automatically be updated. Disable JavaScript. Uninstall Java from the computer. Deny all first-party and third-party cookies. Block all plug-ins and unsandboxed plug-ins. Never save passwords in the browser. Set the browser to clear all browsing automatically when it is closed. Identify and install security browser extensions that will provide extended protection. Only surf in private mode. Turn on the pop-up blocker.

SECURE WEB EMAIL—Set up two recovery options. The first is to a smartphone, while the second is to a remote email account that is used for no other purpose than to receive recovery reset information from an account. Monitor the main email account

regularly for any suspicious activity. Periodically reset the web email password. Never click a hyperlink contained in an email. Do not open any email attachments, even those received from a known sender. Instead, use a secure web file transfer facility when transferring files.

Chapter Summary

- The Internet is a worldwide network of computer networks. These networks are operated by industry, governments, schools, and even individuals who all loosely cooperate. The World Wide Web (WWW) is composed of Internet server computers on networks that provide online information in the Hypertext Markup Language (HTML) format. Instructions written in HTML code specify how a local computer's web browser should display the various elements of a webpage. Web servers distribute HTML documents based on a set of standards known as the Hypertext Transport Protocol (HTTP). Email systems use either the Simple Mail Transfer Protocol (SMTP) to handle outgoing mail and the Post Office Protocol 3 (POP3) for incoming mail or the Internet Mail Access Protocol (IMAP).
- Solutions for providing dynamic web content come in different forms. One solution requires special scripting computer code to be downloaded and executed in the user's web browser. JavaScript is the most popular scripting code. There are different defense mechanisms intended to prevent JavaScript programs from causing harm; however, there still are security concerns with using JavaScript. Extensions expand the normal capabilities of a web browser for a specific webpage. Extensions are browser-dependent, so that an extension that works in one brand of web browser will not function in another. A plug-in adds new functionality to the web browser so that users can play music, view videos, or display special graphical images within the browser. Plug-ins serve as the link to external programs that are independent of the browser. Add-ons add a greater degree of functionality to the entire browser and not just to a single webpage as with a plug-in. Extensions, plug-ins, and add-ons can all be security risks.
- Attackers have turned to using these third-party advertising networks to distribute their own malware to unsuspecting users who are visiting a well-known website. This is known as malvertising. Ads containing malware secretly redirect visitors to the attacker's webpage that then downloads malware through vulnerabilities in the browser or browser additions. Instead of infecting through third-party advertising, network attackers can also infect the website directly through drive-by downloads.
- A cookie is a file that a web server stores on the local computer that contains user-specific information. A first-party cookie is created from the website that a user is currently viewing, while a third-party cookie is created by another entity that is different from the primary website. A locally shared object (LSO) is a special cookie used with Adobe Flash. A Flash cookie is named after the Adobe Flash player. Cookies can pose both security and privacy risks.

- One of the more common means of distributing attacks is through email. Spam, or unsolicited email, is widely used to distribute malware. Another common means of distributing attacks is through email attachments, or files that are sent with an email message. These files can contain malware and can infect a user's computer when they are opened. Email messages often contain embedded hyperlinks, which are contained within the body of the message as a shortcut to a website. Attackers can take advantage of embedded hyperlinks to direct users to the attacker's website.
- There are different defenses that can be used to protect against Internet attacks. One defense is properly configuring the security settings on the web browser, which allows the user to customize security and privacy settings. Almost all major web browsers support security-related browser additions, such as extensions, plug-ins, and add-ons. These may provide an additional level of security.
- There are security defenses that can be configured to protect against attacks through email. Spam filters can block spam that has bypassed other filters. Most email clients contain a reading pane that allows the user to read an email message without actually opening it. Email clients can also be configured to block external content in HTML email messages that are received, such as hyperlinks to pictures or sounds. When accessing webmail through a web browser there are also security settings to be considered. Because email attachments can contain malware, it is important to be wary regarding these types of files. Attachment protection is also becoming available in other applications.
- There are several Internet security best practices when using a web browser or accessing email. Users should be cautious when downloading files and should control cookies on their computers. They should also delete the browsing history, maintain pop-up blockers, and clear their cache regularly.

Key Terms

Definitions for key terms can be found in the Glossary for this text.

add-on
attachment
blacklist
browser
cookie
drive-by download
embedded hyperlink
extension
first-party cookie
HTML5
Hypertext Markup Language (HTML)
Hypertext Transfer Protocol (HTTP)
image spam
Internet
Internet Mail Access Protocol (IMAP)
Java
JavaScript
locally shared object (LSO)
malvertising
plug-in
Post Office Protocol (POP)
Protected View
reading pane
Simple Mail Transfer Protocol (SMTP)
spam
spam filter
third-party cookie
Transmission Control Protocol/Internet Protocol (TCP/IP)
whitelist
World Wide Web (WWW)

Review Questions

1. Each of the following is true about the Internet except:
   a. It is not controlled by a single organization or government entity.
   b. It is a local network of computers and networks.
   c. Industry, governments, schools, and individuals all loosely cooperate in the Internet's self-governance.
   d. It is composed of networks to which devices are attached.
2. What is the format used to write webpages?
   a. Hypertext Transport Protocol (HTTP)
   b. Hypertext Markup Language (HTML)
   c. Transmission Control Protocol/Internet Protocol (TCP/IP)
   d. Microsoft Adobe Printer (MAP)
3. Which of the following is the more recent and advanced electronic email system?
   a. Simple Mail Transfer Protocol (SMTP)
   b. Transmission Control Protocol (TCP)
   c. Post Office Protocol (POP)
   d. Internet Mail Access Protocol (IMAP)
4. Which is the most popular scripting code used with webpages?
   a. Java
   b. JavaScript
   c. Hypertext Markup Language (HTML)
   d. Hypertext Transport Protocol (HTTP)
5. Each of the following is an addition that could be added to a web browser to support dynamic browsing except _____.
   a. Java
   b. extension
   c. add-ons
   d. plug-ins
6. A cookie that was not created by the website that attempts to access it is called a _____.
   a. first-party cookie
   b. second-party cookie
   c. third-party cookie
   d. resource cookie

7. Which of the follow web browser additions provides links to external programs?
   a. Java applet
   b. plug-in
   c. extension
   d. add-on
8. How does an attacker use a malvertising attack?
   a. Attackers directly infect the website that is being compromised by identifying a vulnerability in the web server.
   b. Java applets are attached to spam messages that pretend to be advertisements.
   c. Attackers may infect the third-party advertising networks so that their malware is distributed through ads sent to user's web browsers.
   d. Resource objects are sent as email attachments with a source that pretends to be a well-known advertising agency.
9. A _____ is a list of email addresses from senders from whom you do not want to receive messages.
   a. whitelist
   b. blacklist
   c. greenlist
   d. redlist
10. Which of the following is true about a cookie?
    a. It can contain a virus.
    b. It can pose a security and privacy risk.
    c. It acts like a worm.
    d. It places a small file on the web server computer sent from the browser.
11. Bob's computer was infected from a drive-by download attack. What did Bob do to get infected?
    a. He opened an email attachment.
    b. He viewed a website.
    c. He unknowingly sent a virus to a website.
    d. He clicked *Download*.
12. Which type of cookie is the most complex?
    a. locally shared object (LSO)
    b. plug-in cookie
    c. control cookie (CC)
    d. extender cookie (CE)

13. What technique do attackers use in order to circumvent text-based spam filters?
    a. object spam
    b. attachment spam
    c. Flash spam
    d. image spam
14. What is the first step in defending against Internet-based attacks?
    a. Use a web browser that supports automatic downloads.
    b. Ensure that the computer itself is properly secured.
    c. Do not open email attachments.
    d. Add security extensions to the web browser.
15. Why should you not click on an embedded hyperlink?
    a. They are slow.
    b. They seldom work properly.
    c. They can take you to a different website other than what is being advertised.
    d. They can take up too much disk space on your computer.
16. A reading pane allows the user to read an email message _____.
    a. after the attachment has been saved to the hard drive
    b. only one time
    c. without actually opening it
    d. from a remote location
17. The most secure option when configuring a web browser for security is _____.
    a. accept first-party cookies.
    b. accept first-party cookies but deny third-party cookies.
    c. reject locally shared objects but accept second-party cookies.
    d. deny first-party and third-party cookies.
18. Which of the following is not a web browser addition to enhance security?
    a. website reputation
    b. local intranet flash signal
    c. URL expander
    d. plug-in validation
19. Why would you want to block external content from downloading into your email client?
    a. To prevent spammers from knowing that your email address is valid
    b. To take advantage of the remote reading pane
    c. To slow down your email client so you can read the message
    d. To prevent your computer's graphics processor utility buffer from filling too quickly

20. Which of the following is not a secure Internet practice?
    a. Restrict cookies in web browsers through browser settings.
    b. Double-check spelling on a typed web address before submitting.
    c. Do not click on embedded hyperlinks in an email.
    d. Run JavaScript code to prevent attacks.

Hands-On Projects

Project 4-1: Test Browser Security

One of the first steps in securing a web browser is to conduct an analysis to determine if any security vulnerabilities exist. These vulnerabilities may be a result of missing patches or out-of-date plug-ins. In this project, you will use a plug-in to scan the Firefox or Chrome browser.

1. Open the Firefox or Chrome web browser and enter the URL *browsercheck.qualys.com* (if you are no longer able to access the site through the web address, use a search engine to search for "Qualys BrowserCheck").
2. Click **FAQ**.
3. Read the information on this page about what the Qualys BrowserCheck plug-in will do.
4. Return to the home page.
5. Click **Install Plugin**.
6. Check the box **I have read and accepted the Service User Agreement.**
7. Click **Continue**.
8. Follow your browser's instructions to install the plug-in.
9. After the plug-in is installed, a Qualys button will appear at the top of the browser. Click on the button.
10. A message appears indicating that you must also install the Qualys BrowserCheck host application. Follow the instructions to download the host application.
11. Launch the host application when the download is complete. Follow the default instructions to install the host application.
12. When the host application installation is complete restart your browser.
13. Click the Qualys button.
14. The plug-in will begin to scan your browser.
15. An analysis of the browser's security will appear, like that shown in Figure 4-8.
16. If there are any security issues detected, click the **Fix It** buttons to correct the problem. Follow the instructions on each page to correct the problems.

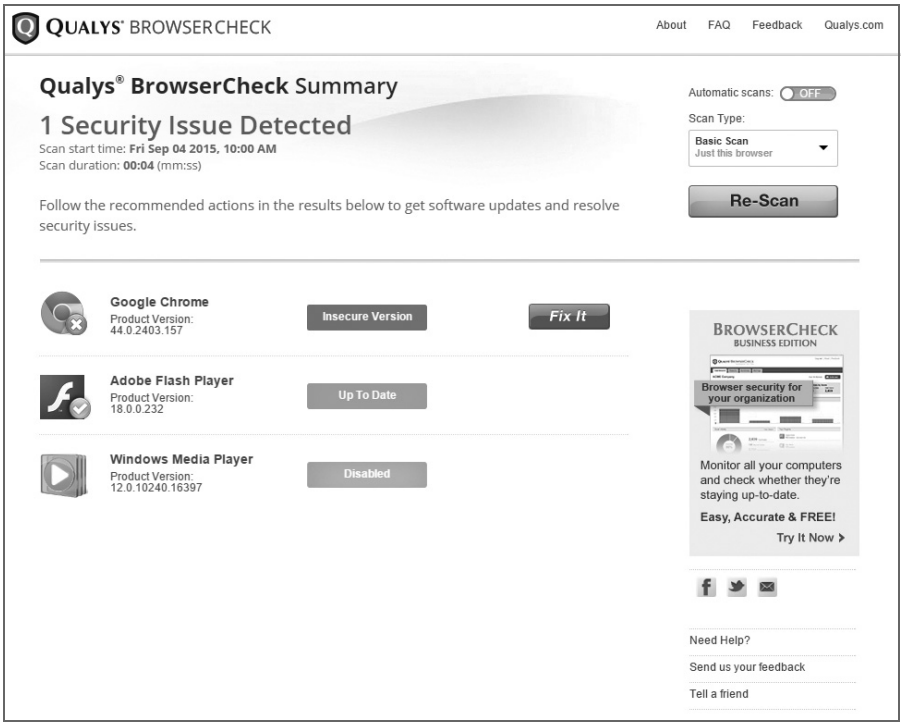


Figure 4-8 Browser security scan results

Source: Qualys Browser

17. Return to the Qualys scan results page.
18. Under **Scan Type**, click **Advanced Scan** and then click **Re-Scan**. This will scan all browsers on the computer and also check the Microsoft patches that have been installed.
19. When the scan is finished click each of the tabs (**Browser/Plugins**, **System Checks**, and **MS Updates**) for each of the browsers listed. Be sure to correct any security problems.
20. Close all windows.

Project 4-2: Manage Locally Shared Objects

A locally shared object (LSO) is an enhanced cookie used by Adobe Flash and other applications. These cookies cannot be deleted through the browser's normal configuration settings as regular cookies can. Instead, they are managed through the Adobe website for your computer. In this project, you will change the settings on LSOs.

1. Use your web browser to go to *www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager07.html* (if you are no longer able to access the site through the web address, use a search engine to search for "Flash Player Help").
2. The Adobe Flash Player Settings Manager panel is displayed as shown in Figure 4-9.

Figure 4-9 Adobe Flash Player Settings Manager panel

Source: Adobe

3. The first tab is the Global Privacy Settings for Camera and Microphone. Click the first tab to display the settings.
4. Click **Always ask …** so that you are prompted when a website wants to access your camera or microphone through Adobe Flash. Click **Confirm**.
5. Click the next tab, which is the **Global Storage Settings**. Uncheck **Allow third-party Flash content to store data on your computer**.
6. Click the next tab, which is the **Global Security Settings** tab. Be sure that either **Always ask** or **Always deny** is selected.
7. Click the **Website Privacy Settings** tab. This regards privacy settings for a camera or microphone for sites that you have already visited in the past. Click **Delete all sites** and then **Confirm**.
8. Close all windows.

Project 4-3: Alternative Web Browser—Privacy

Besides the major web browsers there are several other web browsers available that are tuned for enhanced security or privacy. In this project, you will download an alternative web browser that is tuned for privacy.

1. Use your web browser to go to *www.browzar.com/* (if you are no longer able to access the site through the web address, use a search engine to search for "Browzar private web browser").
2. Click **Download now–it's FREE**

3. Under **Black Theme** click **Download.**
4. Click **Accept.**
5. Click **Download.**
6. Save the file to the desired location on your computer.
7. When the download has completed navigate to the **BrowzarBlack2000.exe** file and double-click on it to launch the Browzar web browser.

Browzar does not need to be installed and can run from a USB flash drive.

8. Click **Tools.**
9. Click **Secure Delete…**
10. Click **Enable.**
11. Use Browzar to navigate to several different websites that you frequent.
12. Enter a search term in the **Private Search …** toolbar. This enables a search of the web with no traces left behind of that search term.
13. Close Browzar. What appears on the screen as the browser performs its clean-up operation? How can this improve your privacy?

Project 4-4: Web Browser Security Settings

In this project, you will configure several security settings for the Google Chrome web browser and assess the impact of the settings.

1. Launch the Google Chrome web browser.
2. Go to *amazon.com* and search for different items of your interest. Add several to the Amazon shopping cart. When finished close Chrome.
3. Launch Chrome again and return to *amazon.com*.
4. Look at the Amazon shopping cart. Are your items still available? Why?
5. Now visit several other websites. Notice that the ads that are displayed are of similar items that you searched for on Amazon. Why did this happen? When finished close Chrome.
6. Launch Chrome.
7. Click the "hamburger" icon and then click **Settings** to display the Chrome settings.
8. Click **Show advanced settings …**
9. Under **Privacy** click **Content settings …**
10. Under **Cookies** click **All cookies and site data …**

11. Scroll through the list of cookies on your computer. Can you determine which cookies are from third-party advertising networks?
12. Click a site listed that has stored a cookie on your computer.
13. Click on the name of the cookie to display the contents.
14. Click **Done** or **Finished**.
15. Click **Done** or **Finished** again to return to the **Settings** menu.
16. Now remove all the cookies by clicking **Clear browsing data …**
17. Under **Obliterate the following items from:** change to **the beginning of time**.
18. Click **Clear browsing data**.
19. Under **Privacy** click **Content settings …**
20. Under **Cookies** click **Block sites from setting any data**.
21. Click **Block third-party cookies and site data.**
22. Now block JavaScript. Scroll down to **JavaScript** and click **Do not allow any site to run JavaScript**.
23. Force Chrome to ask your permission to run plug-ins. Under **Plug-ins** click **Let me choose when to run plug-in content**.
24. Click **Done** or **Finished**.
25. Close this Chrome tab.
26. Return to **amazon.com** and search for different items of your interest as you did before. Add several to the Amazon shopping cart. When finished close Chrome.
27. Launch Chrome again and return to *amazon.com*.
28. Look at the Amazon shopping cart. Are your items still available? What happened?
29. Now visit several other websites. What do you notice about the ads that displayed now? Why?
30. Close all windows.

Case Projects

Case Project 4-1: Compare Browser Security

Of the most popular web browsers—IE, Firefox, Safari, Opera, and Chrome—which is the most secure? Using the Internet, research the security features of each of these browsers. Create a table that lists the different security features. In your opinion, is there one browser that is more secure than the rest? Is there a browser that is the least secure? Give reasons for your conclusion.

Case Project 4-2: Information Security Community Site Activity

The Information Security Community Site is an online companion to this textbook. It contains a wide variety of tools, information, discussion boards, and other features to assist learners. Go to *community.cengage.com/infosec*. Sign in with the login name and password that you created in Chapter 1.

How would you restrict spam? Should it be done by technology or passing laws (remember that domestic laws would not apply to spammers who lived outside the country)? Should all spammers be required to register with a central agency? What should be the penalty for violating your proposal? Record your responses on the Community Site discussion board.

Additional Case Projects for this chapter are available through the MindTap online learning environment.

References

1. "Email Market, 2015-2019," *The Radicati Group*, accessed Aug. 30, 2015. http://www.radicati.com/wp/wp-content/uploads/2015/07/Email-Market-2015-2019-Executive-Summary.pdf.
2. "Plugin Directory," *WordPress*, accessed Aug. 30, 2015. https://wordpress.org/plugins/.
3. "Cisco 2015 Midyear Security Report," *Cisco*, accessed Aug. 30, 2015. http://www.cisco.com/web/offers/lp/2015-midyear-security-report/index.html.
4. Pauli, Darren, "Malware Menaces Poison Ads as Google, Yahoo! Look Away," *The Register*, accessed Sep. 1, 2015. http://www.theregister.co.uk/2015/08/27/malvertising_feature/?page=1.
5. Evans, David, "Flash Will Soon Be Obsolete: It's Time for Agencies to Adapt," *Advertising Age*, Jun. 11, 2015, accessed Sep. 3, 2015. http://adage.com/article/digitalnext/flash-obsolete-time-agencies-adapt/298946/.
6. Korolov, Maria, "The Web's Ten Most Dangerous Neighborhoods," *CSO*, Sep. 1, 2015, accessed Sep. 3, 2015. http://www.csoonline.com/article/2978317/data-protection/the-webs-ten-most-dangerous-neighborhoods.html.

chapter 5

Mobile Security

After completing this chapter you should be able to do the following:

- Describe attacks through Wi-Fi and Bluetooth networks
- Explain the different types of attacks on mobile devices
- List the defenses for a home Wi-Fi network
- Describe how to use a public wireless network securely
- List the types of security for mobile devices

Security in Your World

Braden shifted his backpack and rang the doorbell. "Hi, Braden. I'm afraid that Gabe isn't back from school yet," Mrs. Sullivan said as she opened the door. Braden lived next door to the Sullivans in a quiet neighborhood, and he and Mrs. Sullivan's son Gabe, who had been friends since elementary school, both were now attending the local college where Braden was majoring in computer information systems. "That's OK. I really came over here to show you something," Braden said.

Mrs. Sullivan looked puzzled. "Please, come in. What is it?" Braden slipped his laptop computer out of his backpack and opened it. He explained that at the college he was studying wireless network security in his Wireless Technology course this semester. The project for this week was to download two free wireless applications from the Internet and use them. "This first program," said Braden, "finds Wi-Fi wireless networks that don't have any security. Look. Just right here in our neighborhood there are 17 Wi-Fi networks this program can detect, and 5 of them are unprotected." Mrs. Sullivan looked at the computer screen and said, "Well, OK. Is that what you came over here to show me?"

Braden set the laptop on the table and said, "Sort of. I was in the kitchen at our house when I started this program. And it showed that your Wi-Fi network was one of those that was not secured. See? Look at this line SULLIVAN_HOUSE. I'm guessing that's your home Wi-Fi network because it's got your name in it." Mrs. Sullivan looked at Braden's computer screen and said, "Yes, I see that. But I'm afraid I still don't understand what you wanted to show me." Braden took a deep breath and said, "Mrs. Sullivan, from inside my house I was able to pick up the signal from your Wi-Fi network. So I launched this second program. And I could see what you were doing on your computer that was going over your network."

Mrs. Sullivan leaned forward. "Wait a minute. You mean that from over at your house you could see this? I thought the walls of our house blocked any signal from getting out." Braden shook his head and said, "No, they don't. And you need to see this. I captured it on my computer." Braden moved the laptop and showed Mrs. Sullivan her network data that he had captured while at his house. Mrs. Sullivan gasped. She saw lines of an email message that she had been typing on her computer just minutes before Braden came over. "And," Braden continued, "if you had been typing passwords or credit card numbers I might have seen those, too."

Mrs. Sullivan looked very concerned. She occasionally worked from home and used her new tablet connected to their home Wi-Fi network. "Could anybody else see this?" she asked. "Yes," said Braden, "unless the network is protected, anybody who can pick up your signal can see what you're doing. And when I walked over here I walked down our street and could pick up your signal the entire time. So anybody out on the street could see this."

Mrs. Sullivan stood up. "Braden, you've got me very worried. How do we fix this?"

The word *ubiquitous* means "ever-present" or "found everywhere." And that is an accurate description of wireless data networks and the mobile devices that connect to these networks. Thanks to smartphones, tablets, and laptops, and the wireless networks behind them, it is no longer necessary to use a desktop computer tethered by cable to a network in order to surf the web, check email, or access company inventory records. Mobile devices and wireless networks have made mobility possible to a degree rarely even imagined before. Travelers use their mobile devices to access the Internet while waiting at airports, traveling on airplanes and trains, and working in their hotel rooms. At work, businesses have found that employees who have wireless access to data during meetings and in conference rooms can significantly increase their productivity. Free wireless Internet connections are expected today by customers in coffee shops, by students on college campuses, and by fans in arenas and stadiums. There is hardly a part of our world that has not been dramatically affected by mobile devices and wireless technology.

Statistics confirm the popularity of wireless networks and mobile devices. Users now spend over half of their computing time each day using a mobile device compared to 42 percent on a desktop computer (as recently as 2008 almost 80 percent of time was spent exclusively on a desktop). Four out of every five web searches today are performed first on a mobile device.[1] And users have become increasingly attached to their devices. A new dictionary word has recently been introduced to reflect this: *nomophobia* is the fear of being without your mobile phone!

But just as users have flocked to mobile devices and wireless networks, so too have attackers. Mobile devices have seen an increase in malware and attacks directed at them. Wireless data networks also have become a prime target for attackers who attempt to capture the unprotected wireless signal freely floating through the air in order to uncover passwords, credit card numbers, and other important information. Just as it is important for users to protect their desktop computers, it is also critical to protect their mobile devices and wireless networks.

In this chapter, you will examine some of the attacks on mobile devices and the wireless data networks that support them. First, you will explore the types of attacks that a wireless network faces along with the attacks directed at mobile devices using these networks. Then, you will learn how to protect wireless networks at home and how to use public wireless networks safely. You will also look at how to protect the mobile devices themselves.

Mobile Attacks

There are several types of attacks that are directed toward mobile devices. And understanding the attacks directed toward wireless networks that support these devices is equally important.

Attacks through Wireless Networks

There are two major types of wireless networks that are popular today and they also are targets for attackers. These networks are Wi-Fi and Bluetooth.

Wi-Fi Networks Wi-Fi networks have become commonplace today. Understanding what Wi-Fi is, the equipment needed to operate on a Wi-Fi network, and the attacks that this type of network faces are all important.

What Is Wi-Fi? **Wi-Fi** (*wireless fidelity*) is a wireless data network technology that provides high-speed data connections for mobile devices. This type of network is technically known as a **wireless local area network** (**WLAN**) and is intended to replace or supplement a wired local area network (LAN). Devices such as tablets, laptop computers, smartphones, and wireless printers that are within 460 feet (140 meters) of a centrally located connection device can send and receive information using radio frequency (RF) transmissions at speeds that typically range from 54 million bits per second (Mbps) to as high as 7 billion bits per second (Gbps).

Wi-Fi networks are different from the cellular telephony networks that are designed, installed, and maintained by the wireless telephone carriers. These networks use standards such as *3G* and *4G LTE* for both voice and data communications and charge users accordingly for this coverage. Wi-Fi networks, in comparison, are set up and maintained by users and are faster than cellular telephony networks although they have a smaller geographical area of coverage.

In the field of computer networking and wireless communications, the most widely known and influential organization is the **Institute of Electrical and Electronics Engineers** (**IEEE**). The IEEE and its predecessor organizations date back to 1884. The IEEE is one of the leading developers of global standards in a broad range of industries such as energy, biomedical and healthcare, and transportation, and is currently involved in developing and revising over 800 standards. The IEEE has been responsible for establishing standards for Wi-Fi networks. Table 5-1 lists the different standards and their characteristics.

Characteristic	802.11	802.11b	802.11a	802.11g	802.11n	802.11ac
Frequency	2.4 GHz	2.4 GHz	5 GHz	2.4 GHz	2.4 & 5 GHz	5 GHz
Nonoverlapping channels	3	3	23	3	21	21
Maximum data rate	2 Mbps	11 Mbps	54 Mbps	54 Mbps	600 Mbps	7.2 Gbps
Indoor range (feet/meters)	65/20	125/38	115/35	115/35	230/70	115/35
Outdoor range (feet/meters)	328/100	460/140	393/120	460/140	820/250	460/140
Standard ratification date	1997	1999	1999	2003	2009	2014

Table 5-1 **IEEE WLAN standards**

Wi-Fi Equipment The list of equipment needed for a Wi-Fi wireless network is surprisingly short. Each mobile device (laptop, tablet, smartphone, etc.) must have a **wireless client network interface card adapter** (or *wireless adapter*) to send and receive the wireless signals. Although early wireless adapters were external devices that connected to the computer's Universal Serial Bus (USB) and had an external antenna, today they are internal and built into mobile devices. In addition to this wireless adapter, special software is needed that translates data between the wireless adapter and the device. All operating systems today include this software that will automatically scan the airwaves, detect any Wi-Fi networks in the area, and either offer the user the option of connecting to that network or automatically connect based on previous preferences set by the user.

The other equipment needed for a home-based Wi-Fi network actually combines several networking technologies. Strictly speaking these devices are *residential WLAN gateways* as they are the entry point from the Internet into the Wi-Fi network. However, most vendors instead choose to label their products as *wireless broadband routers* or more commonly, **wireless routers**. The wireless router acts as the "base station" for the wireless devices, sending and receiving wireless signals between all devices as well as providing the "gateway" to the external Internet (it typically is connected to the user's modem that is in turn connected to an Internet connection). A wireless router is illustrated in Figure 5-1.

Figure 5-1 Wireless router

A home Wi-Fi network is shown in Figure 5-2. The RF transmission signal from the wireless router allows the laptop and tablet to wirelessly connect to it. The wireless router in turn is connected to all other network devices as well as the Internet. Because the wireless router supports both wired devices (PC and printer) as well as wireless devices (laptop and tablet), this

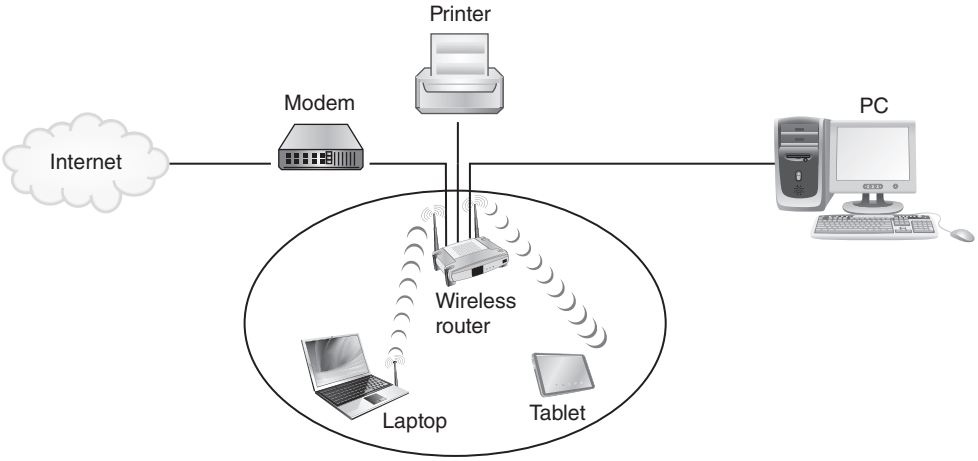


Figure 5-2 Home Wi-Fi network

enables all the devices to equally share resources. For example, the wireless tablet can print to the wired printer, and all wired and wireless devices can share the single Internet connection.

In a business or school setting, instead of using a single wireless broadband router, a more sophisticated device known as an **access point** (**AP**) is used. Whereas most homes or apartments would have only one wireless router, businesses typically have multiple APs (often into the hundreds). Because the wireless signal can only be transmitted for several hundred feet, multiple APs are used to provide "cells" or areas of coverage. As the user moves (called *roaming*) from one cell to another with their wireless device, a *handoff* occurs so that the AP to which the user is closest now becomes the new base station. Cells of coverage are shown in Figure 5-3.

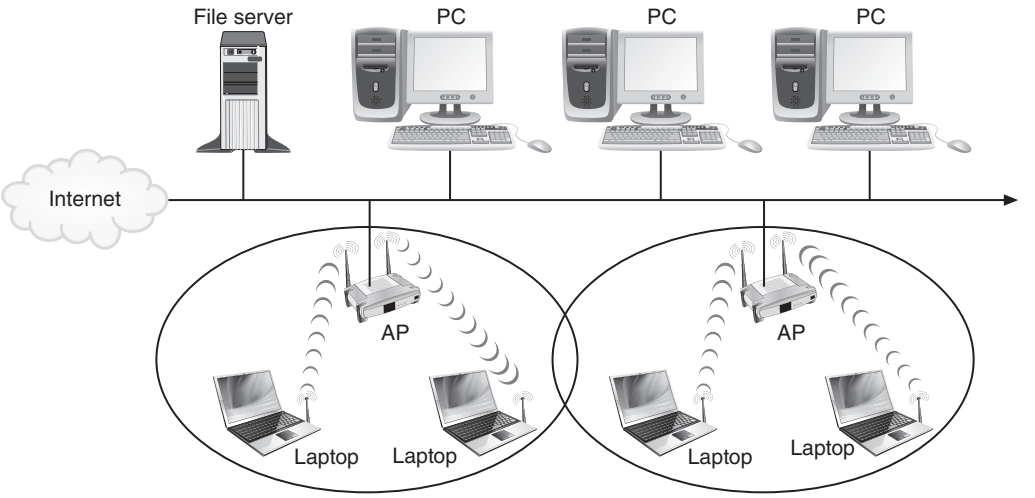


Figure 5-3 Wi-Fi cells

Attacks on Wi-Fi Home users face several risks from attacks on their Wi-Fi networks, such as:

- *Reading wireless transmissions*. Usernames, passwords, credit card numbers, and other information sent over the Wi-Fi network could be easily seen by an attacker.
- *Viewing or stealing computer data*. An attacker who is able to connect to a home Wi-Fi network could access *any* folder that has file sharing enabled on *any* computer on the network. This essentially provides an attacker full access to view or steal sensitive data from all computers on the network.
- *Injecting malware*. Because attackers might access the network behind a firewall, they could inject Trojans, viruses, and other malware onto the user's computer.
- *Downloading harmful content*. In several instances, attackers have accessed a home computer through an unprotected Wi-Fi network, downloaded child pornography to the computer, and then turned that computer into a file server to distribute the content. When authorities traced the files back to that computer, the unsuspecting owner was arrested and his equipment confiscated.

Attackers can easily identify unprotected home wireless networks through **war driving**. War driving is searching for wireless signals from an automobile or on foot using a portable

computing device. Free software is readably available on the Internet to detect unprotected networks and read the data that is being transmitted over the wireless network.

War driving is derived from the term *war dialing*. When telephone modems were popular in the 1980s and 1990s, an attacker could program the device to randomly dial telephone numbers until a computer answered the call. This random process of searching for a connection was known as war dialing, so the phrase for randomly searching for a wireless signal became known as war driving.

When using a public Wi-Fi network in a coffee shop, airport, or school campus there are also security concerns. First, these networks are rarely protected (in order to allow easy access by users), so attackers can read any wireless transmissions sent to and from the user's device. In addition, an attacker may set up an **evil twin**. An evil twin is an AP or another computer designed to mimic an authorized Wi-Fi device. A user's mobile device may unknowingly connect to this evil twin instead of the authorized device so that attackers can receive any sensitive transmissions or directly send malware to the user's computer.

Attacks against home Wi-Fi networks are considered to be relatively easy, for several reasons. First, most home users overlook the fact that the signal emanating from a wireless router is not confined to the house or apartment and can be picked up outside of the building, in some cases hundreds of feet away. This enables an unseen attacker to silently access the wireless network or view transmissions. Second, many home users are unaware how to configure security on their router. Third, some users simply are unaware of the risks of an unprotected Wi-Fi network.

Bluetooth

Bluetooth is another widespread wireless technology. Bluetooth is a short-range wireless technology designed for quick "pairing" or interconnecting of two or more devices together, such as a laptop computer with a Bluetooth mouse. Examples of Bluetooth-enabled product pairings are listed in Table 5-2. Unlike Wi-Fi that can provide coverage of up to several hundred feet at fast speeds, most Bluetooth devices have a range of only 33 feet (10 meters). Also, the rate of transmission is only 1 Mbps.

Category	Bluetooth pairing	Usage
Automobile	Hands-free car system with cell phone	Drivers can speak commands to browse the cell phone's contact list, make hands-free phone calls, or use its navigation system.
Home entertainment	Stereo headphones with portable music player	Users can create a playlist on a portable music player and listen through a set of wireless headphones or speakers.
Photography	Digital camera with printer	Digital photos can be sent directly to a photo printer or from pictures taken on one cell phone to another phone.
Computer accessories	Computer with keyboard and mouse	A small travel mouse can be linked to a laptop or a full-size mouse and keyboard that can be connected to a desktop computer.
Gaming	Video game system with controller	Gaming devices and video game systems can support multiple controllers, while Bluetooth headsets allow gamers to chat as they play.
Medical and health	Blood pressure monitors with smartphones	Patient information can be sent to a smartphone, which can then send an emergency phone message, if necessary.

Table 5-2 Bluetooth products

The current version is Bluetooth v4.2, but all Bluetooth devices are backward compatible with previous versions.

Bluetooth is also finding its way into unlikely devices. A Bluetooth-enabled basketball monitors the forces applied to it, from spin to dribble, and provides feedback to a Bluetooth smartphone or tablet regarding the player's performance. Another Bluetooth device alerts an ice fisherman's smartphone when a fish brushes her fishing line beneath the ice.

Because of the "on-the-fly" nature of Bluetooth pairings, attacks on wireless Bluetooth technology are not uncommon. Two Bluetooth attacks are bluejacking and bluesnarfing. **Bluejacking** is an attack that sends unsolicited messages to Bluetooth-enabled devices. Usually bluejacking involves sending text messages, but images and sounds can also be transmitted. Bluejacking is usually considered more annoying than harmful because no data is stolen. However, many Bluetooth users resent receiving unsolicited messages. **Bluesnarfing** is an attack that accesses unauthorized information from a wireless device through a Bluetooth connection, often between cell phones and laptop computers. In a bluesnarfing attack, the attacker copies emails, calendars, contact lists, cell phone pictures, or videos by connecting to the Bluetooth device without the owner's knowledge or permission.

Attacks on Mobile Devices

In addition to attacks on the wireless networks to which mobile devices are connected, attacks on the devices themselves are also common. There are different types of mobile devices, and there are security risks associated with using these devices.

Types of Mobile Devices

There are a variety of different types of mobile devices. These include portable computers, tablets, smartphones, and wearable technology.

Portable Computers

As a class, *portable computers* are devices that closely resemble standard desktop computers. These portable computers have similar hardware (keyboard, hard disk drive, RAM, etc.) and run the same operating systems (Windows, Apple Mac OS, or Linux) and application software (Microsoft Office, web browsers, etc.) that are found on a general-purpose desktop computer. The primary difference is that portable computers are smaller self-contained devices that can easily be transported from one location to another while operating on battery power.

The first commercially successful portable computer was the Osborne 1, released in 1981. Its screen was only 5 inches (13 centimeters), and it had a single floppy disk drive. Weighing in at a hefty 23.5 pounds (10.7 kg), it was said to be more "luggable" than portable.

A relatively new class of portable computers is the *subnotebook* computer, sometimes called an *ultrabook* (Intel/Windows) or *air* (Apple). These devices are even smaller than standard portable computers and use low-power processors and advanced solid-state hard disk drives. Figure 5-4 shows a subnotebook computer.

Figure 5-4 Subnotebook computer

A new type of computing device that resembles a laptop computer is a *web-based computer*. It contains a limited version of the Linux operating system and a web browser with an integrated media player. Web-based computers are designed to be used primarily while connected to the Internet. No traditional software applications can be installed, and no user files are stored locally on the device. Instead, the device accesses online web apps and saves user files on the Internet.

An example of a web-based computer is the Google Chromebook, which costs significantly less than a full-featured laptop computer.

Because portable computers use the same hardware and run the same software as standard desktop computers, they face the same risks of attack by viruses, worms, Trojans, rootkits, etc. An additional risk is that these portable computers also are subject to theft or loss.

Tablets **Tablets** are portable computing devices that are generally larger than smartphones and smaller than laptops, and are focused on ease of use. Tablets generally lack a built-in keyboard and instead rely on a touch screen. Tablets are often classified by their screen size. The two most common categories of tablet screen sizes are 5–8.5 inches (12.7–21.5 cm) and 8.5–10 inches (12.7–25.4 cm). The weight of tablets is generally less than 1.5 pounds (0.68 kg), and they are less than 1/2 inch (1.2 cm) thick. Figure 5-5 shows a typical tablet computer.

Designed for user convenience, tablets are thinner, lighter, easier to carry, and more intuitive to use than portable computers. Whereas portable computers are designed for performance, tablets are primarily display devices that can accommodate limited user input. Tablet computers have an operating system that allows them to run other software

Figure 5-5 Tablet computer

programs (called *apps*). The most popular operating systems for tablets are Apple iOS, Google Android, and MicrosoftWindows Mobile.

Tablets are purchased more often in mature markets like the United States, while laptops sell better in emerging markets. This is because laptops are often the only computing devices in a household in emerging markets, whereas in mature markets tablets supplement existing computer resources.

Smartphones A *feature phone* is a traditional cellular telephone that includes a limited number of features, such as a camera, an MP3 music player, and ability to send and receive *short message service (SMS)* text messages. Many feature phones are designed to highlight a single feature, such as the ability to take high-quality photos or provide a large amount of memory for music storage.

A **smartphone** has all the tools that a feature phone has but also includes an operating system that allows it to run apps and access the Internet. Because it has an operating system, a smartphone offers a broader range of functionality. Users can install apps that perform a wide variety of functions for productivity, social networking, music, and so forth, much like a standard computer. In fact, because of this ability to run apps, smartphones are essentially handheld personal computers. As the popularity of smartphones has increased, the sales of feature phones have decreased. Two out of every three mobile phones today are smartphones, totaling over 1.2 billion smartphones sold each year.[2]

Despite its small screen size, one-third of all videos are watched on smartphones.[3]

Wearable Technology A new class of mobile technology consists of devices that can be worn by the user instead of carried. Known as **wearable technology**, these devices can provide even greater flexibility and mobility. As the cost of wearable technology has decreased

while the network speed of the devices has increased, sales of this technology have dramatically risen. Wearable device shipments worldwide totaled 26 million units in 2014 and increased 173 percent the following year to 72 million units. It is estimated that wearable device shipments worldwide will reach 175 million by 2020.[4]

The most common type of wearable technology is a *fitness tracker*, as shown in Figure 5-6. These devices typically monitor movements by counting steps and distance traveled, record heart rates, provide location data, give alerts of incoming email, calls, or text messages, and even monitor sleep patterns.

Figure 5-6 Fitness tracker

Whereas standard fitness trackers can display results directly on the device itself, the lower-cost budget trackers will only display progress on a smartphone app.

Another type of wearable technology is a *smartwatch*. This device can serve as an accessory to a smartphone so that users can easily glance at the watch to view messages without the need to remove the smartphone from a bag or pocket. The device also may have its own set of sensors and software features to function independently. For example, it could serve as a control device for home automation systems.

One of the first wearable technologies was an optical head-mounted display, sometimes called a "wearable computer." These could be activated in response to the user's voice commands or tilting the head 30 degrees upward. Then a specific voice command (called a "voice action") could be given, such as requesting directions (*Give me directions to Tampa, Florida*), issuing a command to make a web search (*Google Cengage Learning*), or an action to use one of the device's features (*Take a picture* or *Record a video*). However, these devices are not in widespread use.

Mobile Device Risks There are several security risks associated with using mobile devices. These include installing insecure applications, limited physical security, connecting to public networks, location tracking, and accessing untrusted content.

Installing Unsecured Applications Software for traditional desktop computers is generally purchased from large and reputable vendors or is developed in-house within an organization. In contrast, mobile devices are designed to easily locate, acquire, and install apps from a variety of sources. These sources range from large reputable vendors to single-person developers and even hobbyists. Many apps are free while others can be purchased at a nominal cost. In many cases, however, these apps do not include security features.

Currently, there are two dominant operating systems for mobile devices, Apple iOS and Google Android, on which the apps function. These two operating systems are very different and have different levels of security.

Two other operating systems for mobile devices are Microsoft Windows Mobile and BlackBerry. The market share for these products, however, is currently very small.

The Apple **iOS** operating system, developed by Apple for its mobile devices, is a closed and proprietary architecture. This makes it much more difficult for attackers to create an app that could compromise it and become a security risk. In addition, iOS uses its App Store, which is part of Apple iTunes, as the sole source for distributing apps. iTunes is Apple's "mobile ecosystem" infrastructure that is used to download apps, organize them, and even play digital audio and video on personal computers and other Apple products (iPod Touch, iPhone, iPad, etc.). All iOS apps must first be reviewed and approved by Apple before they can be made available on the App Store. This allows Apple to screen for malicious apps and prevent them from being posted.

With more than 1 million apps in the App Store, however, mobile app developers face stiff competition to have their app recognized and generate revenue. As a result, many app developers generate supplementary revenue by selling user data generated through the app to third-party advertising networks and analytics companies. In addition, this user data collected by the app and sent back to the developer for distribution is transmitted in such a way so that an attacker could access it.

Unlike Apple iOS, the Google **Android** operating system for mobile devices is not proprietary but is entirely open for anyone to use or even modify. Apps for Android devices can be downloaded from the Google Play store (which does not screen apps like Apple does) or can be downloaded from an unofficial third-party website (called **sideloading**).

Generally, this makes Android apps highly risky. One report says that the number of malicious Android apps worldwide increased by an additional 350,000 in a six-month period. Most of these malicious apps are imitations of legitimate popular apps or are Trojans. About 44 percent of these malicious apps are designed to trick users into downloading costly services, such as sending expensive text messages (with the malware developer receiving a portion of the charges). Other malicious Android apps steal user data (24 percent) or load adware (17 percent).[5]

Limited Physical Security The greatest asset of a mobile device—its portability—is also considered its greatest vulnerability. Mobile devices are used in a wide variety of locations (schools, restaurants, coffee shops, hotels, etc.) that are outside of the user's home. Devices can easily be lost or stolen, and any unprotected data on the device could be retrieved by the thief.

In addition to loss or theft, merely using a mobile device in a public area can be considered a risk. Users must constantly guard against strangers looking over their shoulders who want to view sensitive information being displayed on the device or view a user's password as it is being entered.

Connecting to Public Networks Mobile devices must use public external networks for their Internet access. Because these networks are beyond the control of the user, the type of security that is available may be suspect. If proper security is not implemented, attackers can eavesdrop on the data transmissions and view sensitive information.

Location Tracking Mobile devices with *global positioning system (GPS)* capabilities typically run **location services**. These services can identify the location of a person carrying a mobile device or a specific store or restaurant. This enables the location of a friend to be identified or the address of the nearest coffee shop to be displayed. Location services are used extensively by social media, navigation systems, weather systems, and other mobile-aware applications. An increasing use of location services is to enable a smartphone to immediately display a coupon whenever a user comes in close proximity to a store or restaurant.

Mobile devices using location services are at increased risk of targeted physical attacks. An attacker can easily determine where the user and the mobile device are currently located and use that information to follow the user in order to steal the mobile device or inflict harm upon the person. In addition, attackers can compile over time a list of people with whom the user associates and the types of activities they perform in particular locations in order to craft attacks.

Accessing Untrusted Content Mobile devices have the ability to access untrusted content that other types of computing devices generally do not have. One example is *Quick Response (QR)* codes. These codes are a matrix or two-dimensional barcode, first designed for the automotive industry in Japan. QR codes consist of black modules (square dots) arranged in a square grid on a white background, which can be read by an imaging device such as a mobile device's camera. A QR code can store website URLs, plain text, phone numbers, email addresses, or virtually any alphanumeric data up to 4296 characters. A QR code for the Cengage Learning website is illustrated in Figure 5-7.

Figure 5-7 QR code

QR codes are internationally standardized.

An attacker can create an advertisement listing a reputable website, such as a bank, but include a QR code that contains a malicious URL. Once the user snaps a picture of the QR code using his mobile device's camera, the code directs the web browser on his mobile device to the attacker's imposter website or to a site that immediately downloads malware.

The heightened risks associated with mobile devices can be seen in how these devices are being used. Almost three out of every five users between 18 and 34 years old use their mobile phones at least once per month to access their bank, credit union, credit card or brokerage account through the phone's browser, app, or text message service. More than half of the entire U.S. adult population use mobile phone banking.[6]

Security in Your World

"That should do it," said Braden. He had just finished helping Mrs. Sullivan configure her wireless router. "Braden, I had no idea there were so many different options on this router," said Mrs. Sullivan. "Look at these." She pointed at the screen and read several of the settings. "This one says 'Fragmentation length.' And what is 'CTS/RTS Threshold' and 'Short preamble mode?' How would anybody know what to do unless they had someone like you to help them?" she asked. Braden moved the mouse and said, "I know what you mean. The problem is that those options you're looking at are about changing how the wireless signals are transmitted. There isn't any reason why anybody would change those unless they're having a transmission issue. But people look at those and can easily get overwhelmed and think that configuring the security on their router is really complicated, so they don't even try."

"And," said Mrs. Sullivan, "I think most people are like me and just don't know what to do about security on their router. But watching you makes me think that it's not that hard. You did it in less than five minutes." Braden smiled and said, "It really isn't hard at all. It just takes a few minutes to make your wireless network safe."

"Braden, I can't thank you enough," said Mrs. Sullivan. "I'm glad to help," Braden replied. "Now, can I show you a couple of things about your new tablet? There are some security settings on it that are good to have turned on. There's a setting for this tablet that does a 'remote wipe' that you might be interested in."

"What's a remote wipe?" asked Mrs. Sullivan. "If you ever lose the tablet or it gets stolen, you can remotely erase your data, so the thief can't get it. Some companies require all of their users to have it on their mobile devices," said Braden.

Mrs. Sullivan leaned forward in her chair. "That is exactly what I need. Can you show me how to install it?"

Mobile Defenses

Despite the fact that there are many different attacks directed at mobile devices and wireless networks, there are several defenses that can be utilized for protection. These defenses can be broken down into defenses for wireless networks and defenses for protecting the wireless devices.

Wireless Network Security

Reducing the risk of attack through wireless networks is an important security step. This involves securing a Wi-Fi home wireless network, following secure practices for using a public wireless network safely, and configuring Bluetooth on devices.

Home Wi-Fi Security Configuring a Wi-Fi wireless router in order to provide the highest level of security protection is an important step. Configuring the router includes securing it and turning on **Wi-Fi Protected Access 2 (WPA2) Personal**. In addition, there are other security settings that can be implemented.

Securing the Wireless Router The first step in securing a Wi-Fi wireless router is essential but is frequently overlooked. It involves "locking down" the device by creating a password to protect its internal configuration settings. Most wireless routers come preconfigured with a default password, and these passwords are well known by attackers. Protecting the router with a strong password prevents attackers from remotely accessing the wireless router and turning off any security settings.

To secure the wireless router, the address of the router and the default password must first be known. This information is included in the documentation of the wireless router, can be obtained through the vendor's website, or can be determined by examining the network settings. The wireless router's Internet Protocol (IP) address, such as *192.168.1.1*, can be entered into a web browser on a computer connected to the wireless network, which then displays the router's login screen. Once the default password is entered, access will be granted to the configuration settings of the router where a new password can be entered.

In addition, most routers also permit remote management of the router's configuration settings through the Internet. There are several router configuration options for remote management. The typical settings, as illustrated in Figure 5-8, are as follows:

- *Enable remote management*. This setting permits users to access the router's configuration settings from another location through the Internet.

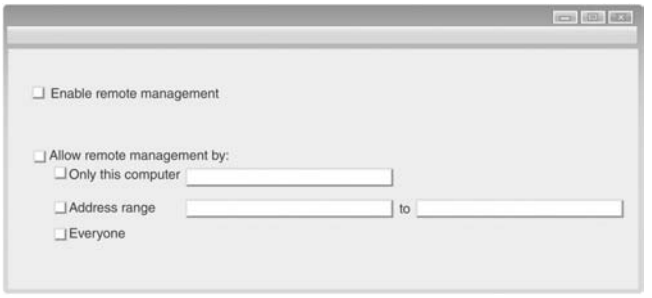


Figure 5-8 Wireless router remote access settings

- *Allow remote management by:*. This option designates which devices can perform remote management. It can be one device (*Only this computer*), multiple devices (*Address range*), or all devices (*Everyone*).

Some newer wireless routers provide remote management and wireless network access via an app installed on a smartphone or tablet. This app lets users check to see if a computer, mobile device, gaming console, media player, or other device is attached to the wireless network. In addition, email alert notifications can be sent to warn owners of a security intrusion attempt into the network or whenever a security update is available.

Unless remote management is essential, it is recommended that this feature be disabled. Turning remote management off adds a stronger degree of security, because it limits access to the configuration settings of the wireless router to only the local computer connected to it.

Turning on Wi-Fi Protected Access 2 (WPA2) Personal The wireless signal that comes from a wireless router can be picked outside of the building where the router is located, in some cases hundreds of feet away. On an unsecured wireless network, virtually anyone can access the Wi-Fi signal to read transmissions and to access the network. This makes it critical to perform two key security tasks: to mask the transmission so that no one can read any information being sent and received and to prevent unauthorized users from accessing the network.

Although these two tasks may seem daunting, they can easily be accomplished by turning on WPA2 Personal. WPA2 provides the optimum level of wireless security and is part of all certified wireless devices. Implementing WPA2 Personal involves turning it on at the wireless router and then entering a key value on each authorized device that has been preapproved to join the Wi-Fi network. In the wireless router configuration settings there are two steps that must be performed. First, the WPA2 Personal security option, which may be labeled as *WPA2-PSK [AES]*, is turned on by clicking the appropriate option button. Second, a key value, sometimes called a *preshared key (PSK)*, *WPA2 shared key*, or *passphrase*, must be entered. This key value can be from 8 to 63 characters in length. An example of the settings dialog box for WPA2 Personal is illustrated in Figure 5-9.

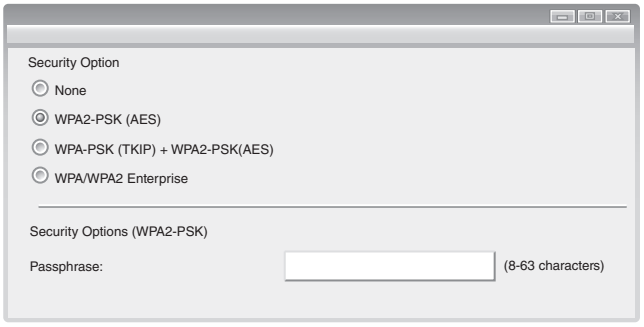


Figure 5-9 WPA2 Personal wireless router settings

After turning on WPA2 Personal on the wireless router and entering a key value, the same key value must also be entered on each mobile device that wants to access the Wi-Fi network. A mobile device that attempts to access a wireless network with WPA2 Personal will automatically ask for the key value. After this value is entered, the device can access the wireless network. And once the key value is entered, the mobile device can retain the value and does not need to ask for it again.

As a means of simplifying WPA2 Personal, many wireless routers support **Wi-Fi Protected Setup** (**WPS**) as an optional means of configuring security. There are two common WPS methods. The PIN method utilizes a personal identification number (PIN) printed on a label on the wireless router or displayed through a software setup wizard. The user types in the PIN on the mobile device (such as a tablet or laptop computer), and the security configuration automatically occurs. The second method is the push-button method: the user pushes a button (usually an actual button on the wireless router and a virtual one displayed through a software setup wizard on the wireless device), and the security configuration takes place. However, it has been revealed that there are significant security design and implementation flaws in WPS using the PIN method. It is recommended that only the manual configuration method be used or that WPS be disabled on the wireless router and then turned on only temporarily when adding a new device to the Wi-Fi network.

Other Security Settings Although securing the wireless router with a strong password and turning on WPA2 Personal are the most effective Wi-Fi security settings, there are other security settings that can add an additional degree of security:

- *Changing the SSID*. The name of the wireless network can be set by the user and is called the *Service Set Identifier (SSID)*. All wireless routers come with a default SSID. An attacker who picks up a Wi-Fi signal and can read the SSID will immediately know the type of wireless router being used and can exploit any weaknesses of that type of router. The SSID on the wireless router should be changed from its default value to an anonymous value that does not identify the owner or location of the network. For example, *SULLIVAN_HOUSE* or *1234_Main_St* would not be good SSIDs; a better choice might be something like *MyWireNet599342*.

- *Turning on guest access*. Most wireless routers allow for a separate guest network to be set up in addition to the main Wi-Fi network. This serves to isolate the main network from the guest network. The guest network can be configured so that any user who connects to the separate guest network can only access the Internet directly and other devices in the same network. Another option restricts guests to only Internet access; they cannot access any other network devices, such as a printer.

Although widely advertised, there are other security settings that only provide a slight degree of additional security or no additional security at all. These include *disabling SSID broadcasts, restricting users by MAC address,* and *limiting the number of users*. It is not recommended that these settings be used.

Using Public Wi-Fi Public Wi-Fi networks, such as those in a coffee shop, library, restaurant, or airport, should be used with caution. Because the signals are rarely if ever protected, any attacker in the area can easily read any transmissions. The following is a list of sound practices when using public Wi-Fi:

- *Watch for an evil twin*. Attackers will often impersonate a legitimate Wi-Fi network by creating their own look-alike network, tempting unsuspecting users to connect with the attacker's network instead. Many attackers create a direct *ad hoc network*, a peer-to-peer network that connects a wireless device directly to another wireless device, such as the victim's laptop directly to the attacker's laptop. For example, an attacker who sets up an ad hoc network may name it *Free Wireless Network* or *Free Airport Wireless* in the hopes that an unsuspecting user will connect directly to the attacker's computer. Once the connection is made, the attacker can inject malware into the user's computer or steal data from it. One defense is to note that the icons for an ad hoc network are different from the icons for a network using a wireless router. This is illustrated in Figure 5-10.

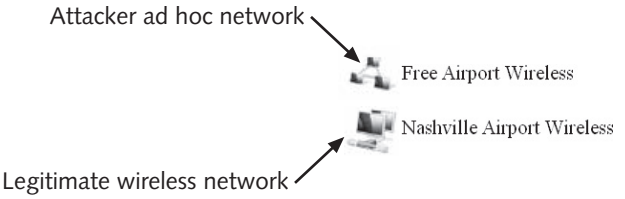


Figure 5-10 Evil twin ad hoc network

- *Limit the type of activity*. It is not advisable to use a public Wi-Fi network for much more than simple web surfing or watching online videos. Accessing online banking sites or sending confidential information such as a Social Security number could be intercepted by an attacker if not properly protected.
- *Use a virtual private network*. A **virtual private network (VPN)** uses an unsecured public network, such as the Internet, as if it were a secure private network. It does

this by encrypting all data that is transmitted between the remote device and the network. This ensures that any transmissions that are intercepted will be indecipherable. VPNs can be software-based or hardware-based. Software-based VPNs, in which the VPN software is running on the mobile device itself, are common. A wireless user can "tunnel" through the less-than-secure public Wi-Fi network using a VPN, relying on its security advantages. For example, a user may access a public wireless hotspot at an airport or coffee shop and use VPN to "tunnel" through it to reach a secure corporate network.

Configuring Bluetooth When using a smartphone or tablet that supports Bluetooth, it is advisable to disable Bluetooth and turn on this service only as necessary. To prevent bluesnarfing, Bluetooth devices should be turned off when not being used or when in a room with unknown people. Another option is to set Bluetooth on the device as *undiscoverable*, which keeps Bluetooth turned on in a state where it cannot be detected by another device.

Mobile Device Security

Securing mobile devices requires several steps. These include the initial setup of the device, following best practices, and dealing with the theft or loss of the device.

Device Setup Several configurations should be considered when initially setting up a mobile device. These include disabling unused features and enabling screen locks.

Disable Unused Features Mobile devices include a wide variety of features for the user's convenience. However, each of these can also serve as a threat vector. It is important to disable unused features and turn off those that do not support the business use of the device or that are rarely used. One of the features that should be disabled if it is not being regularly used is Bluetooth wireless data communication in order to prevent bluejacking and bluesnarfing.

Enable a Lock Screen A **lock screen** prevents the mobile device from being used until the user enters the correct passcode, such as a PIN, password, swipe pattern on the screen, or fingerprint touch ID. Lock screens should be configured so that whenever the device is turned on or is left idle for a period of time, the user must enter the passcode. Most mobile devices can be set to have the screen automatically lock after anywhere from 30 seconds to 30 minutes of inactivity.

A lock screen is a different setting from the *sleep time* setting that regulates when the device goes into a hibernation mode.

Some mobile devices can be configured so that after a specific number of failed attempts to enter the correct passcode, such as when a thief is trying to guess the code, additional security protections will occur, including:

- *Extend the lockout period*. If an incorrect passcode is entered a specific number of times, the lockout period will be extended. For example, if the incorrect passcode is entered five consecutive times, the mobile device will remain completely locked for one minute. If the incorrect code is entered again after one minute, the device will stay locked for double that time, or two minutes. For each successive incorrect entry, the lockout period will double.
- *Reset to factory settings*. If an incorrect passcode is entered a set number of times, the user will be prompted to enter a special phrase to continue. If the phrase is correctly entered, then the user will have only one more opportunity to enter the correct passcode. If an incorrect passcode is entered again, the device will automatically reset to its factory settings and erase any data stored on it.

Most mobile devices have different options for the type of passcode that can be entered. The most secure option is to configure a strong alphanumeric password on the mobile device. Another option is to draw or swipe a specific pattern connecting dots, as illustrated in Figure 5-11.

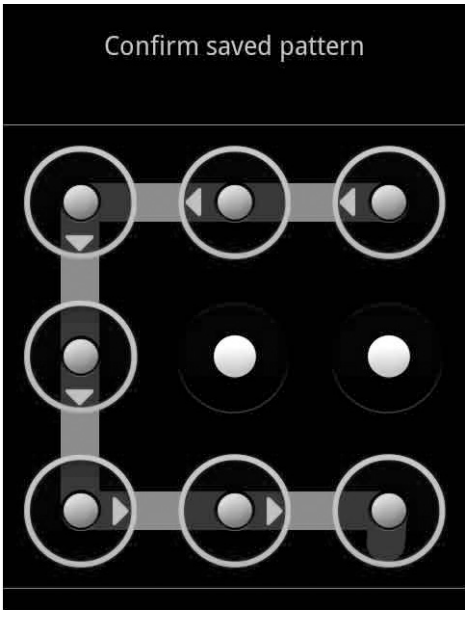


Figure 5-11 Swipe pattern

Source: OnlineAndroidTips.com

The least effective method is a short PIN. Many users opt to set a short four-digit PIN, similar to those used with a bank's automated teller machine (ATM). However, short PIN codes provide only a limited amount of security. An analysis of 3.4 million users' four-digit (0000–9999) PINs that were compromised revealed that users create predictable PIN patterns. The PIN *1234* was used in more than 1 out of every 10 PINs. Table 5-3 lists the five most common PINs and their frequency of use. Of the 10,000 potential PIN combinations, 26.83 percent of all PINs could be guessed by attempting just the top 20 most frequent PINs.[7]

PIN	Frequency of use
1234	10.71%
1111	6.01%
0000	1.88%
1212	1.19%
7777	0.74%

Table 5-3 Most common PINs

The research also revealed that the least common PIN was *8068*, which appeared in only 25 of the 3.4 million PINs.

Best Practices A list of "best practices" for using mobile devices securely includes the following:

- Users may be tempted to erase the installed built-in limitations on their smartphone (called **jailbreaking** on Apple iOS devices or **rooting** on Android devices) to provide additional functionality. However, because this also disables the built-in operating system security features on the device, this should not be practiced.
- Do not sideload unapproved apps.
- Use appropriate sanitization and disposal procedures for mobile devices. Users should delete all information stored in a mobile device before discarding, exchanging, or donating it.
- Back up data stored on the mobile device on a regular basis.
- Do not call telephone numbers contained in unsolicited emails or text messages.
- Be aware of current threats affecting mobile devices.

Device Loss or Theft One of the greatest risks of a mobile device is the loss or theft of the device. Unprotected devices can be used to access user web resources or view sensitive data stored on the device. In order to reduce the risk of theft or loss:

- Keep the mobile device out of sight when traveling in a high-risk area.
- Avoid becoming distracted by what is on the device. Always maintain an awareness of your surroundings.
- When holding a device, use both hands to make it more difficult for a thief to snatch.
- Do not use the device on escalators or near transit train doors.
- White or red headphone cords may indicate they are connected to an expensive device. Consider changing the cord to a less conspicuous color.
- If a theft does occur, do not resist or chase the thief. Instead, take note of the suspect's description, including any identifying characteristics and clothing, and then call the authorities. Also contact the organization or wireless carrier and change all passwords for accounts accessed on the device.

If a mobile device is lost or stolen, several different security features can be used to locate the device or limit the damage. Many of these can be used through either a feature in the operating system or an installed third-party app. These features are listed in Table 5-4.

Security feature	Explanation
Alarm	The device can generate an alarm even if it is on mute.
Last known location	If the battery is charged to less than a specific percentage, the device's last known location can be indicated on an online map.
Locate	The current location of the device can be pinpointed on a map through the device's GPS.
Remote lockout	The mobile device can be remotely locked and a custom message sent that is displayed on the login screen.
Thief picture	A thief who enters an incorrect passcode three times will have her picture taken through the device's onboard camera and emailed to the owner.

Table 5-4 Security features for locating lost or stolen mobile devices

If a lost or stolen device cannot be recovered, it may be necessary to perform **remote wiping**, which will erase the data stored on the mobile device. This ensures that even if a thief is able to access the device, no sensitive data will be compromised.

Exceptional Security

LOCK DOWN THE WIRELESS ROUTER—Use an industrial-grade wireless router instead of a consumer-edition product. Protect the wireless router with a strong password, do not enable remote management, turn on WPA2, and turn off WPS. Use a cryptic SSID that cannot be directly traced to the owner or a specific location. Only turn on guest access when it is needed, then turn it off once guests leave. Do not use public Wi-Fi for any activity for which sensitive data is exchanged. Set up a VPN when using an unsecured Wi-Fi network.

PROTECT SMARTPHONES AND TABLETS—Do not take pictures of QR codes. Turn off location services on mobile devices. When traveling, save all important files to an online storage repository and not on a laptop's hard drive or USB flash drive, which may be compromised if lost or stolen. Only turn on Bluetooth when it is needed, then turn it off again. Create a lock screen that uses a strong password and not a PIN or uses a swipe pattern or touch ID. Never jailbreak or root a mobile device. Do not side-load apps. Back up cell phone data on a regular basis to another device, then wipe out unnecessary data. Be cautious when using a mobile device in a crowded public area. Set up and become familiar with remote wiping apps available for the device.

Chapter Summary

- Wi-Fi is a wireless data network technology that provides high-speed data connections for mobile devices. The Institute of Electrical and Electronics Engineers (IEEE) has been responsible for establishing standards for Wi-Fi networks. Each mobile device must have a wireless client network interface card adapter to send and receive the wireless signals, and these are built into mobile devices. In addition, a wireless router is needed for a home-based Wi-Fi network. This router acts as the "base station" for wireless devices, sending and receiving wireless signals between all devices as well as providing the "gateway" to the external Internet. In an office setting, instead of using a wireless router, a more sophisticated device, known as an access point (AP), is used.
- There are several different attacks that can launched against home Wi-Fi networks, such as stealing data, reading wireless transmissions, injecting malware, and downloading harmful content. In a public Wi-Fi network an attacker can set up an evil twin to mimic an authorized Wi-Fi device. A user's mobile device may unknowingly connect to this evil twin instead of the authorized device so that attackers can receive any transmissions or directly send malware to the user's computer or device.
- Bluetooth technology is a short-range wireless technology designed for interconnecting of two or more devices. Two Bluetooth attacks are bluejacking and bluesnarfing. Bluejacking is an attack that sends unsolicited messages to Bluetooth-enabled devices. Bluesnarfing is an attack that accesses unauthorized information from a wireless device through a Bluetooth connection, often between cell phones and laptop computers.
- There are a variety of different types of mobile devices. Portable computers are devices that perform much like standard desktop computers but are smaller, self-contained devices that can easily be transported from one location to another while operating on battery power. Because portable computers use the same hardware and run the same software as standard desktop computers, they face the same risks of attack by viruses, worms, Trojans, rootkits, etc., while an additional risk is that portable computers also are subject to theft or loss. Tablets are portable computing devices that are generally larger than smartphones and smaller than laptops and are focused on ease of use. A smartphone has an operating system that allows it to run apps and access the Internet. A new class of mobile technology consists of devices that can be worn by the user instead of carried. Known as wearable technology, these devices can provide even greater flexibility and mobility.
- Several risks are associated with using mobile devices. Mobile devices are designed to easily locate, acquire, and install apps from a variety of sources; however, in many cases, these apps do not include security features. Mobile devices are used in a wide variety of locations that are outside of the home, and this opens the door for these devices to easily be lost or stolen, and any unprotected data on the device can be retrieved by a thief. Mobile devices must use public external networks for Internet access. Because these networks are beyond the control of the user, the type of security that is available may be questionable. Mobile devices with GPS capabilities can run location services to identify the location of a person carrying a mobile device. This places the user at an increased risk of targeted physical attacks. Mobile devices have the ability to access untrusted content that other types of computing devices generally do not have.

- Configuring a Wi-Fi wireless router to provide the highest level of security protection is an important step in securing a wireless network. The first step in securing a Wi-Fi wireless broadband router involves "locking down" the device by creating a password to access its internal configuration settings. In addition, most routers also permit remote management of the router's configuration settings through the Internet. Unless remote management is essential, it is recommended that this feature be disabled.
- Another important step in securing a Wi-Fi network is turning on Wi-Fi Protected Access 2 (WPA2) Personal security. Turning on WPA2 Personal involves turning it on at the wireless router and then entering a key value on each authorized device that has been preapproved to join the Wi-Fi network. As a means of simplifying turning on WPA2 Personal, many devices now support Wi-Fi Protected Setup (WPS) as an optional means of configuring security; however, there are vulnerabilities in WPS. Although securing the wireless router with a strong password and turning on WPA2 Personal are the most effective Wi-Fi security settings, there are other security settings that are widely promoted. Unfortunately, some of these only provide a marginal degree of additional security or no additional security at all.
- Public Wi-Fi networks, such as those in a coffee shop, library, restaurant, and airport, should be used with caution. Because the signals on public Wi-Fi networks are rarely if ever encrypted, any attacker in the area can easily read any transmissions. When using a smartphone or tablet that supports Bluetooth it is advisable to disable Bluetooth and turn on this service only as necessary.
- Several configurations should be considered when initially setting up a mobile device for use. These include disabling unused features and enabling lock screens. In addition, "best practices" for using mobile devices securely should be followed. If a mobile device is lost or stolen, several different security features can be used to locate the device or limit the damage. Many of these can be used through either a feature in the operating system or an installed third-party app.

Key Terms

Definitions for key terms can be found in the Glossary for this text.

access point (AP)
Android
bluejacking
bluesnarfing
Bluetooth
evil twin
Institute of Electrical and Electronics Engineers (IEEE)
iOS
jailbreaking
location services
lock screen
remote wiping
rooting
sideloading
smartphone
tablet
virtual private network (VPN)
war driving
wearable technology
Wi-Fi (wireless fidelity)
Wi-Fi Protected Access 2 (WPA2) Personal
Wi-Fi Protected Setup (WPS)
wireless router
wireless client network interface card adapter
wireless local area network (WLAN)

Review Questions

1. The technical name for a Wi-Fi network is:
   a. wireless personal area network (WPAN)
   b. wireless local area network (WLAN)
   c. Bluetooth
   d. wireless ultraband (WU)
2. Tablet computers are designed for _____.
   a. processing capabilities
   b. ease of use
   c. wireless connection speed
   d. hardware upgrades
3. Which of the following is false about a wireless router?
   a. It sends and receives wireless signals between all wireless devices.
   b. It is usually found in a large business with hundreds of wireless users.
   c. It typically is connected to the user's modem.
   d. It combines several networking technologies.
4. When a user moves from one cell of coverage to another cell in a Wi-Fi network this is called _____.
   a. migrating
   b. traveling
   c. roaming
   d. handshaking
5. Which of the following is not a risk that someone would face using an unprotected home Wi-Fi network?
   a. An attacker could steal sensitive data from a computer on the wireless network.
   b. Malware could be injected into computers connected to the Wi-Fi network.
   c. An attacker could take control of the user's keyboard over the network.
   d. The information contained in wireless transmissions could be captured and read.
6. What is one reason Android devices are considered to be at a higher security risk than iOS devices?
   a. All Android apps are free.
   b. iOS has been available longer and has more of its vulnerabilities worked out.
   c. Android apps can be sideloaded.
   d. Apple apps are written in a more secure binary language.

7. _____ is an attack that sends unsolicited messages to Bluetooth-enabled devices.
   a. Bluestealing
   b. Bluejacking
   c. Bluesending
   d. Bluesnarfing
8. Which of the following devices does not have an operating system that allows it to run third-party applications?
   a. tablet
   b. feature phone
   c. smartphone
   d. laptop
9. What prevents a mobile device from being used until the user enters the correct passcode?
   a. swipe identifier (SW-ID)
   b. keyboard
   c. touchpad
   d. lock screen
10. Alice has attempted to enter the passcode on her mobile device but keeps entering the wrong code. Now she is asked to enter a special phrase to continue. This means that her mobile device is configured to _____.
    a. use PIN codes as passcodes
    b. reset to factory settings
    c. extend the lockout period
    d. double the amount of time she is prevented from accessing her device
11. _____ is the process of bypassing the built-in limitations and protections of a mobile device.
    a. Cracking
    b. Twisting
    c. Jailbreaking
    d. Slicing
12. Why should you not sideload apps from an unofficial app store?
    a. Apps are always inferior on an unofficial app store.
    b. It always takes longer to download the app than from an approved store.
    c. It deprives the developers of any royalties.
    d. The apps on these sites are generally not previewed and may contain malware.

13. What is the first step in securing a Wi-Fi wireless broadband router?
    a. creating a password to protect its internal configuration settings
    b. disabling all wireless connections
    c. turning on short preamble packets
    d. monitoring the Wi-Fi signal with a remote telemonitor
14. What provides the optimum level of wireless security for a home Wi-Fi network?
    a. placing the wireless router in a box
    b. using a good identifier
    c. turning on Wi-Fi Protected Setup (WPS)
    d. turning on Wi-Fi Protected Access 2 (WPA2) Personal
15. The primary design of a(n) _____ is to capture the transmissions from legitimate users.
    a. rogue access point
    b. Wireless Equivalent Privacy (WEP)
    c. evil twin
    d. Bluetooth grabber
16. Which of the following can add a stronger degree of security to a Wi-Fi network?
    a. disable SSID broadcasts
    b. restrict users by MAC address
    c. limit the number of users
    d. turn on guest access
17. Each of the following is a sound security practice when using a public Wi-Fi network except _____.
    a. watching out for an evil twin
    b. using the network for less than one hour per day
    c. using a virtual private network (VPN)
    d. not using a public network when entering confidential information on a website
18. Which of the following is not a step to reduce the risk of theft or loss of a mobile device?
    a. recording the MAC address of the device before using it
    b. keeping the mobile device out of sight when traveling in a high-risk area
    c. using both hands to hold a device, making it more difficult for a thief to snatch
    d. not using the device on escalators or near transit train doors

19. _____ protects a mobile device when it has not been used for a set period of time.
    a. Auto-lock
    b. Screen refresh
    c. Manager tie down (MTD)
    d. Remote security
20. Which of the following is *not* a best practice for using a mobile device?
    a. Back up data stored on the mobile device on a regular basis.
    b. Do not jailbreak a mobile device.
    c. Wait 24 hours before reporting a lost device.
    d. Be aware of current threats affecting mobile devices.

Hands-On Projects

Project 5-1: Configuring a Wireless Router Using an Online Emulator

Properly configuring a wireless router is an important task for securing a Wi-Fi network. In this project, you will use the Netgear online emulator to learn the basic steps in configuring a wireless router.

1. Use your web browser to go to **http://www.voiproblem.com/emulators/Netgear/WNR834B/index.html?interface=WNR834B** (if you are no longer able to access the site through the web address, use a search engine to search for "Netgear emulator WNR834B").
2. The first step in securing a Wi-Fi wireless router involves "locking down" the device by creating a password to protect its internal configuration settings. In the left pane under the category **Maintenance** click **Set Password**.
3. The **Set Password** screen appears. In **Old Password** enter the default Netgear password of **password**.
4. In the **New Password** box enter a strong password to prevent attackers from accessing the settings of the wireless router. How many characters in length should this password be? Why?
5. In the **Repeat New Password** enter the password again. Click **Apply**.
6. The next step is to disable remote management so that the configuration settings of the wireless router are available only to the local computer connected to it. In the left pane under the category **Advanced** click **Remote Management**.
7. What is the current status of Remote Management? Is that the proper setting for securing the wireless router? Click **Cancel**.
8. Now Wi-Fi Protected Access 2 (WPA2) Personal should be turned on. In the left pane under the category **Setup** click **Wireless Settings**.

9. Under **Wireless Networks,** enter a name for this network. Remember that a name like SULLIVAN_HOUSE could provide information to attackers regarding the location of this device. What would be a good name for a wireless network where you live? Enter it in the **Name (SSID):** field.
10. Change **Region** to your location.
11. Under **Security Options,** click **WPA2-PSK [AES]** to turn on WPA2 security.
12. The **Security Encryption (WPA2-PSK)** box appears. Under **Passphrase:,** enter a strong and secure phrase to protect the Wi-Fi network. Click **Apply**.

This same passphrase would be entered on each wireless device that has permission to connect to the Wi-Fi network.

13. Now the Wi-Fi network is secure. How difficult were these steps? How long did it take to accomplish it?
14. Close all windows.

Project 5-2: Creating and Using QR Codes

Quick Response (QR) codes can be read by an imaging device, such as a mobile device's camera or online. In this project, you will create and use QR codes to demonstrate the security risks associated with using these codes.

1. Use your web browser to go to **www.qrstuff.com** (if you are no longer able to access the site through the web address, use a search engine to search for "QR Stuff").
2. First create a QR code. Under **DATA TYPE,** be sure that **Website URL** is selected.
3. Under **CONTENT,** enter the URL **http://www.cengagebrain.com**. Note how the **QR CODE PREVIEW** changes.
4. Under **OUTPUT TYPE**, click **DOWNLOAD** to download an image of the QR code.
5. Navigate to the location of the download and open the image. Is there anything you can tell by looking at this code?
6. Now use an online reader to interpret the QR code. Use your web browser to go to **blog.qr4.nl/Online-QR-Code_Decoder.aspx**.
7. Under **Upload QR code image**, click **Choose file**.
8. Navigate to the location of the QR code that you downloaded on your computer and click **Open**.
9. Click **Upload**.
10. What does it display? How could an attacker use a QR code to direct a victim to a malicious website?

11. Return to **www.qrstuff.com**.
12. Click **Google Maps Location** under **DATA TYPE**.
13. Under **Or use the field below to geo-locate an address,** enter an address with which you are familiar. Click **go**.
14. The latitude and longitude will be automatically entered under **CONTENT**.
15. Under **OUTPUT TYPE**, click **DOWNLOAD** to download an image of this QR code.
16. Navigate to the location of the download and open the image. How does it look different from the previous QR code? Is there anything you can tell by looking at this code?
17. Use your web browser to return to **blog.qr4.nl/Online-QR-Code_Decoder.aspx**.
18. Under **Upload QR code image:**, click **Choose file**.
19. Navigate to the location of the Google Maps Location QR code that you downloaded on your computer and click **Open**.
20. Click **Upload**.
21. A URL will be displayed. Paste this URL into a web browser.
22. What does the browser display? How could an attacker use this for a malicious attack?
23. Return to **www.qrstuff.com**.
24. Click each option under **DATA TYPE** to view the different items that can be created by a QR code. Select three and indicate how they could be used by an attacker.
25. Close all windows.

Project 5-3: Download and Install a Wireless Monitor

Most Wi-Fi users are surprised to see just how far their wireless signal will reach, and if the network is unprotected this makes it easy for an attacker hiding several hundred feet away to break into the network. There are several tools available that will show the different wireless signals from Wi-Fi networks that can be detected. In this project, you will download and install the Xirrus Wi-Fi Inspector program. You will need a computer with a wireless network interface card adapter, such as a laptop, to complete this project.

1. Use your web browser to go to **www.xirrus.com/free-tools** (if you are no longer able to access the site through the web address, use a search engine to search for "Xirrus Wi-Fi Inspector").
2. Click **DOWNLOAD WI-FI INSPECTOR**.

Wi-Fi Inspector will run correctly under Windows 10, 8.1, 8.0, 7, and XP.

3. Enter the requested information and click **Download Now**.
4. When finished, launch Wi-Fi Inspector. The Wi-Fi Inspector is laid out in four tiled windows, each displaying different real-time information about the Wi-Fi networks that can be detected. The windows are Radar, Connection, Networks, and Signal History. This is shown in Figure 5-12.

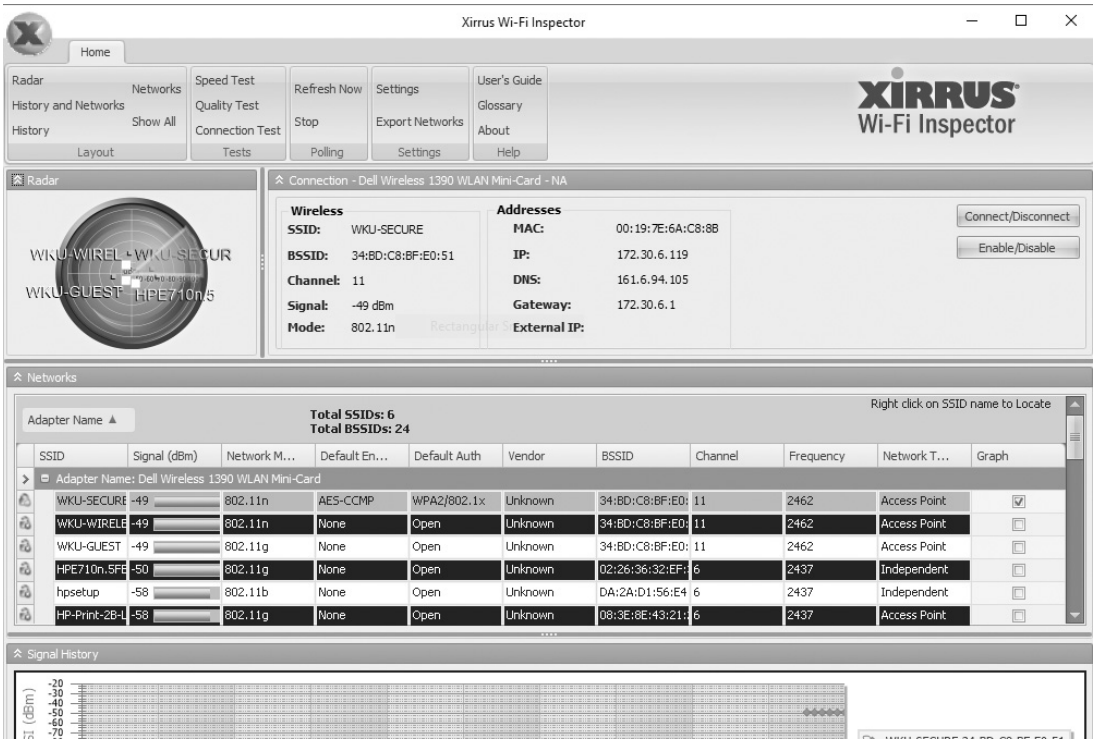


Figure 5-12 Wi-Fi Inspector

Source: Xirrus Wi-Fi Inspector

5. On the **Home** tab, in the **Layout** group, click **Radar** to maximize the radar screen. The Radar screen displays a dynamic view of the Wi-Fi networks in the area. The names of the networks and a corresponding dot are displayed in a circular view, with their relative distance from the center of the radar based on the strength of their Wi-Fi signal (networks from which a strong signal is detected are closer to the center while weaker signals are further away).
6. On the **Home** tab, in the **Layout** group, click **Show All ...** to return to the standard screen layout.
7. In the **Settings** group, click **Settings**.
8. Under **Display Units,** change the setting to **Percent**. Click **Ok**.
9. On the **Home** tab, click **Networks** to maximize the network screen.

10. Scroll through the list of Wi-Fi networks that are detected. Do you recognize all of them as known networks? Click the **Signal (%)** column to show the networks that are the most distant with the weakest signal first. What is the signal strength of the weakest network signal?
11. The Locate Mode can be used to help determine the location of a specific Wi-Fi network. This mode operates similar to a Geiger counter, using sound and visual information to indicate proximity. When in Locate mode, the selected network is highlighted in yellow on the Networks table, it is displayed on the Radar window, and the selected network is graphed in the History window. In addition, an audible beep sounds, the frequency of which reflects signal strength: the quicker the beep, the closer the network.
12. Select a network that has a weak signal and right click on it and select the **Locate** option. While carrying the laptop walk around in your area. How does the radar change? What about the beep sound? Why? How could an attacker use this?
13. To exit Locate mode, right-click on the selected network and select **Exit Locate**.
14. Are you surprised by the number of wireless network signals you can detect? Do you think the different owners of these networks are aware that their signal is accessible?
15. Close all windows.

Project 5-4: Software to Locate a Missing Laptop

If a mobile device is lost or stolen, there are several different security features that can be used to locate the device or limit the damage. Many of these can be used through an installed third-party app. In this project, you will download and install software that can locate a missing laptop computer. Note that for this project a portable computer should be used; however, desktop computer can be used to show the principles of how the program functions.

1. Open your web browser and enter the URL **preyproject.com** (if you are no longer able to access the site through the web address, use a search engine to search for "Prey Project").
2. Click **GET STARTED**.
3. Enter the requested information. Be sure to use a strong password since this application has the ability to track the location of your computer and potentially your location as well. Click **Sign up**.
4. Enter your information to log in.
5. Click **DOWNLOAD PREY**.
6. Select the operating system on the device and Prey will automatically download.
7. When the download is finished, launch the installation program and accept the default settings to install Prey on the computer.

8. On a separate computer, log into your email account to view the message sent by Prey. Click **GO TO MY ACCOUNT** and log into your PreyProject account.
9. Click the name of your recently added device.
10. On the **Devices** tab, select **Sound alarm**. What does this function perform?
11. Click **SET DEVICE TO MISSING** on the **Devices** tab.
12. It may take up to 10 minutes for the alarm to sound, depending on how frequently the device checks into Prey.
13. When a report is generated, click **Reports** and read the information about the location of the device. Would this be sufficient information to find the missing device?
14. Click **SET DEVICE TO RECOVERED** on the **Devices** tab.
15. Close all windows.

Case Projects

Case Project 5-1: Your Wireless Security

Is the wireless network you own as secure as it should be? Examine your wireless network or that of a friend or neighbor and determine which security model it uses. Next, outline the steps it would take to move it to the next highest level. Estimate how much it would cost and how much time it would take to increase the level. Finally, estimate how long it would take you to replace all the data on your computer if it was corrupted by an attacker, and what you might lose. Would this be a motivation to increase your current wireless security model? Write a one-page paper on your work.

Case Project 5-2: Information Security Community Site Activity

The Information Security Community Site is an online companion to this textbook. It contains a wide variety of tools, information, discussion boards, and other features to assist learners. Go to *community.cengage.com/infosec*. Sign in with the login name and password that you created in Chapter 1.

What is the legality of war driving? Is it considered illegal? Why or why not? If it is not illegal, do you think it should be? What should be the penalties? Record your responses on the Community Site discussion board.

Additional Case Projects for this chapter are available through the MindTap online learning environment.

References

1. Bosomworth, Danyl, "Mobile Marketing Statistics 2015", *Smart Insights*, July 22, 2015, accessed Sep. 8, 2015. http://www.smartinsights.com/mobile-marketing/mobile-marketing-analytics/mobile-marketing-statistics.
2. "Gartner Says Smartphone Sales Surpassed One Billion Units in 2014," *Gartner*, Mar. 3, 2015, accessed Sep. 8, 2015. http://www.gartner.com/newsroom/id/2996817.
3. "Mobile Phones Strengthen Lead for Mobile Video Viewing," *eMarketer*, July 2, 2015, accessed Sep. 8, 2015. http://www.emarketer.com/Article/Mobile-Phones-Strengthen-Lead-Mobile-Video-Viewing/1012683?ecid=NL1001.
4. "How Fancy Do Consumers Want Their Wearables?" *eMarketer*, July 21, 2015, accessed Sep. 10, 2015. http://www.emarketer.com/Article/How-Fancy-Do-Consumers-Want-Their-Wearables/1012756.
5. "TrendLabs 2012 Mobile Threat and Security Roundup: Repeating History," accessed Mar. 9, 2014. www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-repeating-history.pdf.
6. "Millennials Embrace Mobile Banking," *eMarketer*, Aug. 18, 2015, accessed Sep. 10, 2015. http://www.emarketer.com/Article/Millennials-Embrace-Mobile-Banking/1012871.
7. "Pin Analysis," *DataGenetics*, accessed Mar. 10, 2014. http://datagenetics.com/blog/september32012/index.html.

chapter 6

Privacy

After completing this chapter you should be able to do the following:

- Define privacy and explain the risks associated with unprotected private data
- Define cryptography
- List the various ways in which cryptography is used
- Explain how privacy best practices may be used
- Describe the responsibilities of organizations regarding protecting private data

Security in Your World

"Good morning, everyone. Let's get started with today's discussion." Dr. Faucheux was teaching the *Current Issues in American Society* course and had assigned students to read three articles for the discussion. "Who wants to start with any reaction to what you read?" he asked.

Amaka raised her hand and said, "I was shocked! I knew that the NSA is supposed to protect us from our enemies. But what they're doing now is against American citizens." The article to which she was referring contained a list of known activities that the U.S. National Security Agency was conducting to monitor American citizens as well as foreign nationals. "Look at this list," Amaka continued. "They can access your email, chat, and web browsing history. They can see what websites you visit. They can track your *Likes* on social media. Where does it all end?"

Bob raised his hand and said, "I don't have a problem with it. They're looking for any terrorists who have sneaked into our country. I want them to find those people before they do anything bad."

Henryk said, "My grandparents had to flee Czechoslovakia and they would tell me about how the government spied on everyone back then. They said you could trust nobody, and nobody trusted you. This sounds a lot like that."

"Let me ask this question," Dr. Faucheux interrupted. "Is this illegal?" Amaka leaned forward and said, "Yes it is. We have a right to privacy in our country." Dr. Faucheux displayed a PowerPoint slide on the screen in front of the classroom. "Here's what the Declaration of Independence says: 'We hold these truths to be self-evident, that all men are created equal, that they are endowed by their Creator with certain unalienable Rights, that among these are Life, Liberty and the pursuit of Happiness.' I don't see privacy listed there, do you?"

"And besides," said Bob, "if you don't have anything to hide, then why would you worry about what they look at? Only criminals need to be afraid."

"Wait a minute," said Henryk. "Didn't the second article we read say that when people were asked, 'Do you have anything to hide?' 83 percent said that they did not. But when they also were asked, 'Would you want to share everything about your life with everyone, everywhere, all the time, forever?' then 89 percent said no. People want their privacy. And the NSA is stealing it."

"Dr. Faucheux, I was thinking along a different line as I read these articles," said Hermione. "Doesn't much of the data collection happen on the websites that we visit? So these websites and the advertising networks are collecting our data? And then it's used in ways we don't even know about and by people we don't even know? Shouldn't we have a say in who collects our online data and how they might use it against us?"

Dr. Faucheux leaned forward in his chair. "Hermione, that's an excellent observation. Class, what do you think about that?"

Over the past 30 years, the changes in our society as a result of the introduction of personal computers and related technology have been nothing short of phenomenal. Advances in medical research, manufacturing systems, transportation, telecommunications, and in many other areas have profoundly impacted the world.

Yet it is universally agreed that an unforeseen consequence of the introduction of technology has also been the erosion of our personal privacy. Whereas in the past individuals could regulate what information about them was gathered and used, today that is no longer the case. Technology has automated the process of the collection of our personal data. The websites we visit, the telephone calls we make, the emails we send, the location of our meeting places, and hundreds of other "data points" about us are collected without our knowledge—and usually without our consent—and then used in a variety of ways. And this data is collected on billions of citizens around the world each day.

Consider just the area of insurance premiums. Does your neighbor pay lower car insurance premiums because data shows that he does not drive between the hours of 2:00 AM and 6:00 AM as you do—even though you are driving to work the early morning shift at that time? Will your health insurance premiums be higher because your web surfing habits show that you are more likely to accept a price increase instead of shopping online for a new policy—even though you work hard to maintain a healthy lifestyle so as to limit the number of your health insurance claims? Are your life insurance premiums higher because a distant relative 50 years ago died at an early age due to a disease—even though you never even knew this person? Are funeral insurance expense policies higher for your lower-income uncle because he visits websites that indicate he struggles with financial literacy and may be confused about insurance—even though he is having difficulty even paying the premiums?

What is even more troubling may be how personal data can be used to change our behavior. Consider Facebook. It has been shown that simply increasing the amount of "hard news" displayed in the Facebook news feeds results in more citizens turning out to vote in elections. Would supporters of a particular candidate running in a close election be able to influence the election results by just increasing the volume of news that is displayed on Facebook news feeds? Or if a Facebook user notices that one of her posts on Facebook about that candidate receives no *Likes* from her friends, she assumes it is because their friends do not agree and she feels silently pressured to support the opposing candidate. But in reality, Facebook simply filtered out her posts from her friends' news feeds so that they never saw the posts. Thus, access to our private data can not only erode our privacy but may also be used to quietly manipulate our behavior.

In this chapter, you learn about privacy and what users can do to protect their data. You will first learn what privacy is and the risks that have been placed on it with today's technology. Then you will examine ways in which to limit the erosion of our privacy.

Privacy Primer

Understanding privacy begins with a definition of privacy. It also involves knowing the risks associated with private data that is collected.

What Is Privacy?

Privacy is defined as *the state or condition of being free from public attention to the degree that you determine*. That is, privacy is freedom from attention, observation, or interference, based on your decision. Privacy is the right to be left alone to the level that you choose.

Prior to the current age of technology, almost all individuals (with the exception of media celebrities and politicians) generally were able to choose the level of privacy that they desired. For those who wanted to have very open and public lives in which anyone and everyone knew everything about them, they were able to freely provide that information about themselves to others. Those who wanted to live a very quiet or even unknown life could limit what information was disseminated. In short, both those wanting a public life and those wanting a private life could choose to do so by controlling information about themselves.

However, today that is no longer possible. Data is collected on almost all actions and transactions that individuals perform. This includes data collected through web surfing, purchases (online and in stores), user surveys and questionnaires, and through a wide array of other sources. It also is collected on benign activities such as the choice of movies streamed through the Internet, the location signals emitted by a cell phone, and even the path of walking as recorded by a surveillance camera. This data is then aggregated by **data brokers**. One data broker holds an average of 1,500 pieces of information on more than 500 million consumers around the world.[1] These brokers then sell the data to interested third parties such as marketers or even governments.

Unlike consumer reporting agencies, which are required by federal law to give consumers free copies of their credit reports and allow them to correct errors, data brokers are not required to show consumers information that has been collected about them or provide a means of correcting it.

Risks Associated with Private Data

The risks associated with the use of private data fall into three categories:

- *Individual inconveniences and identity theft.* Data that has been collected on individuals is frequently used to direct ad marketing campaigns toward the person. These campaigns, which include email, direct mail marketing promotions, and telephone calls, generally are considered annoying and unwanted. In addition, personal data may be used as the basis for identity theft, which involves stealing another person's information (such as Social Security number) and then using the information to impersonate the victim for financial gain. Identity thieves often create new bank or credit card accounts under the victim's name and then charge large purchases to these accounts, leaving the victim responsible for the debts and ruining her credit rating. Usually, identity theft starts with personal data theft.

Identity theft is covered in Chapter 2.

- *Associations with groups*. Another use of personal data is to place what appears to be similar individuals together into groups. One data broker has 70 distinct segments (*clusters*) within 21 consumer and demographic characteristic groups (*life stages*). These groups range from *Boomer Barons* (baby boomer-aged households with high education and income), *Hard Changers* (well-educated and professionally successful singles), and *True Blues* (working parents who hold blue-collar jobs with teenage children about to leave home). Once a person is placed in a group, the characteristics of that group are applied, such as whether a person is a "potential inheritor," an "adult with senior parent," or whether a household has a "diabetic focus" or "senior needs." However, these assumptions may not always be accurate for the individual that has been placed within that group. Individuals might be offered fewer or the wrong types of services based on their association with a group.
- *Statistical inferences*. Statistic inferences are often made that go beyond groupings. For example, researchers have demonstrated that by examining only four data points of credit card purchases (such as the dates and times of purchases) by 1.1 million people, they were able to correctly identify 90 percent of them.[2] In another study, the *Likes* indicated by Facebook users can statistically reveal their sexual orientation, drug use, and political beliefs.[3]

The issues raised regarding how private data is gathered and used are listed in Table 6-1.

Issue	Explanation
The data is gathered and kept in secret.	Users have no formal rights to find out what private information is being gathered, who gathers it, or how it is being used.
The accuracy of the data cannot be verified.	Because users do not have the right to correct or control what personal information is gathered, its accuracy may be suspect. In some cases, inaccurate or incomplete data may lead to erroneous decisions made about individuals without any verification.
Identity theft can impact the accuracy of data.	Victims of identity theft will often have information added to their profile that was the result of actions by the identity thieves, and even this vulnerable group has no right to see or correct the information.
Unknown factors can impact overall ratings.	Ratings are often created from combining thousands of individual factors or data streams, including race, religion, age, gender, household income, zip code, presence of medical conditions, transactional purchase information from retailers, and hundreds more data points about individual consumers. How these different factors impact a person's overall rating is unknown.
Informed consent is usually missing or is misunderstood.	Statements in a privacy policy such as "We may share your information for marketing purposes with third parties" are not clearly informed consent to freely allow the use of personal data. Often users are not even asked for permission to gather their information.
Data is being used for increasingly important decisions.	Private data is being used on an ever-increasing basis to determine eligibility in significant life opportunities, such as jobs, consumer credit, insurance, and identity verification.

Table 6-1 Issues regarding how private data is gathered and used

The inaccuracy of data is of particular concern. A study of consumer financial data used by consumer reporting agencies found that 20 percent of consumers discovered an error on at least one of their three credit reports that had impacted their credit score. After the information was corrected, over 10 percent of consumers saw their credit score increase, while 1 in 20 consumers had a score change of over 25 points. And 1 in 250 consumers who corrected their data had a maximum score change of over 100 points.[4]

The risks associated with private data have led to concern by individuals regarding how their private data is being used. According to a recent survey:[5]

- 91 percent "agree" or "strongly agree" that consumers have lost control over how personal information is collected and used by companies.
- 88 percent "agree" or "strongly agree" that it would be very difficult to remove inaccurate information about them online.
- 80 percent of those who use social networking sites say they are concerned about third parties like advertisers or businesses accessing the data they share on these sites.
- 70 percent of social networking site users say that they are somewhat concerned about the government accessing some of the information they share on social networking sites without their knowledge.
- 62 percent of adults have used a search engine to look up their own name or see what information about them is on the Internet.
- 47 percent generally assume that people they meet will search for information about them on the Internet.
- 16 percent say they have asked someone to remove or correct information about them that was posted online.
- 11 percent of adults say they have had bad experiences because embarrassing or inaccurate information was posted about them online.
- 6 percent have set up some sort of automatic alert to notify them when their name is mentioned in a news story, blog, or elsewhere online.

Security in Your World

"Let's now move to questions from the floor." Dr. Faucheux was serving as moderator of a panel discussion regarding privacy. It was being held by the college's student government association, or SGA. The SGA president, after hearing positive student comments from the *Current Issues in American Society* course, had asked Dr. Faucheux to organize a panel of three different faculty and staff members.

Will raised his hand and said, "I have a question for Mr. Dicello," who taught in the college's marketing department. "Can you explain again how the data the websites get from us is being used?" Mr. Dicello moved toward his microphone and said, "Certainly. The data compiled from the websites that you visit goes far beyond matching products with consumers for determining what ads you will see. It also can be used to set the prices you pay for services like auto insurance. But how those decisions are made isn't clear. There are what we call 'algorithmic black boxes' that are used to make countless important decisions about our lives, but we don't know how they work or even what the algorithm is," he said. "Plus," he continued, "the data that is amassed isn't always accurate or complete, and gives away far more about us than we realize."

Dr. Olhouser from the political science department leaned forward. "We need what I would call a policy approach. It should not be just privacy by design, but privacy by default. But unfortunately, I don't think that public policy and legislation can solve our privacy problem. I'm afraid we'll have to rely on a technology solution."

Mia, who was sitting next to Will, spoke up and said, "What is the technology solution?" Mrs. Jackson, the director of IT at the college, said, "There are browser additions that can help. One popular addition blocks spying ads and invisible trackers. And we also should have end-to-end encryption of everything that is being transmitted and stored. Government agencies can't do mass surveillance if our data is encrypted." Mia raised her hand again and asked, "How does encryption work?"

Privacy Protections

It is virtually impossible today to prevent the collection and use of all private data. Nevertheless, there are several different protections that may be implemented to reduce the risks associated with private data. These protections include using cryptography and following best practices. In addition, organizations that collect private data have responsibilities.

Cryptography

Defining cryptography involves understanding what it is and what it can do. It also involves understanding how cryptography can be used as a tool to protect data.

What Is Cryptography? "Scrambling" data so that it cannot be read is a process known as **cryptography** (from Greek words meaning *hidden writing*). Cryptography is the science of transforming information into a secure form so that unauthorized persons cannot access it.

Whereas cryptography scrambles a message so that it cannot be understood, **steganography** hides the existence of the data. What appears to be a harmless image can contain hidden data, usually some type of message, embedded within the image. Steganography takes the data, divides it into smaller sections, and hides it in unused portions of the file, as shown in Figure 6-1. Steganography may hide data in the file header fields that describe the file,

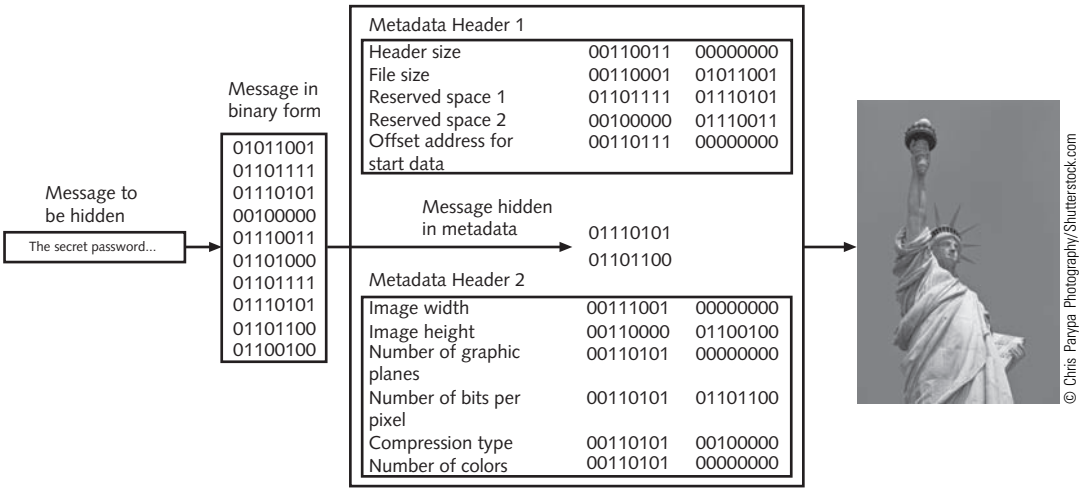


Figure 6-1 Data hidden by steganography

between sections of the *metadata* (data that is used to describe the content or structure of the actual data), or in the areas of a file that contain the content itself. Steganography can use a wide variety of file types—image files, audio files, video files, etc.—to hide messages and data.

Government officials suspect that terrorist groups routinely use steganography to exchange information. A picture of a sunrise posted on a website may actually contain secret information, although it appears harmless.

Cryptography's origins date back centuries. One of the most famous ancient cryptographers was Julius Caesar. In messages to his commanders, Caesar shifted each letter of his messages three places down in the alphabet, so that an *A* was replaced by a *D*, a *B* was replaced by an *E*, and so forth. Changing the original text into a secret message using cryptography is known as **encryption**. When Caesar's commanders received his messages, they reversed the process (such as substituting a *D* for an *A*) to change the secret message back to its original form. This is called **decryption**.

Data in an unencrypted form is called **cleartext** data. Cleartext data is "in the clear" and thus can be displayed as is, without any decryption being necessary. **Plaintext** data is cleartext data that is to be encrypted and is also the result of decryption as well. Plaintext may be considered as a special instance of cleartext.

Plaintext should not be confused with "plain text." Plain text is text that has no formatting (such as bolding or underlining) applied.

Plaintext data is input into a cryptographic **algorithm**, which consists of procedures based on a mathematical formula used to encrypt and decrypt the data. A **key** is a mathematical value entered into the algorithm to produce **ciphertext**, or encrypted data. Just as a key is inserted into a door lock to lock the door, in cryptography a unique mathematical key is input into the encryption algorithm to "lock down" the data by creating the ciphertext. When the ciphertext needs to be returned to plaintext, the reverse process occurs with a decryption algorithm and key. The cryptographic process is illustrated in Figure 6-2.

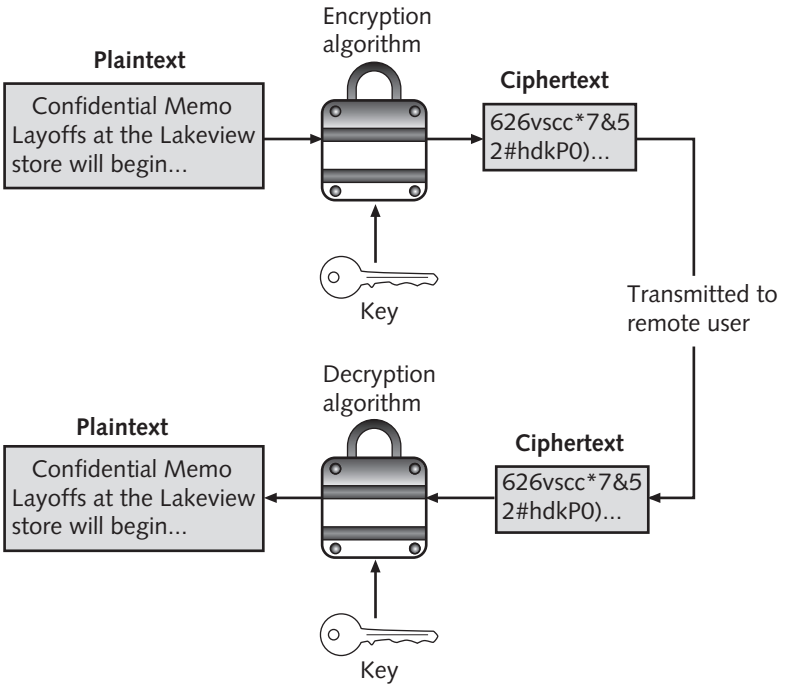


Figure 6-2 Cryptographic process

Cryptography and Privacy Cryptography can provide basic privacy protection for information because access to the keys can be limited. Cryptography can provide five basic protections:

- *Confidentiality*. Cryptography can protect the confidentiality of information by ensuring that only authorized parties can view it. When private information, such as a document containing a user's financial information, is transmitted across the Internet or stored on a USB flash drive, its contents can be encrypted, which allows only authorized individuals who have the key to see it.
- *Integrity*. Cryptography can protect the integrity of information. Integrity ensures that the information is correct and no unauthorized person or malicious software has altered that data. Because ciphertext requires that a key must be used in order to open the data before it can be changed, cryptography can ensure its integrity. The document

of financial information, for example, can be protected so that no data can be added or deleted by unauthorized personnel.

- *Availability*. Cryptography can help ensure the availability of the data so that authorized users who possess the key can access it. Instead of storing an important file on a hard drive that is locked in a safe to prevent unauthorized access, an encrypted file can be immediately available to authorized individuals who have been given the key. The list of document of financial data could be stored on a computer and available to a financial planner for review because she has the algorithm key.
- *Authentication*. The authentication of the sender can be verified through cryptography. Specific types of cryptography, for example, can prevent a situation such as sending a request to a financial planner to withdraw money from an account that appears to come from the user but in reality was sent by an imposter.
- *Nonrepudiation*. Cryptography can enforce nonrepudiation. *Repudiation* is defined as *denial*; nonrepudiation is the inability to deny, so **nonrepudiation** is the process of proving that a user performed an action, such as sending an email message. Nonrepudiation prevents an individual from fraudulently "reneging" on an action. The nonrepudiation features of cryptography can prevent a financial manager from claiming she never sent a copy of financial data transactions to an unauthorized third party.

A practical example of nonrepudiation is Alice taking her car to a repair shop for service and signing an estimate form of the cost of repairs and authorizing the work. If Alice later returns and claims she never approved a specific repair, the signed form can be used as nonrepudiation.

The security protections afforded by cryptography are summarized in Table 6-2. Not all types of cryptography provide all five protections.

Characteristic	Description	Protection
Confidentiality	Ensures that only authorized parties can view the information	Encrypted information can only be viewed by those who have been provided the key.
Integrity	Ensures that the information is correct and no unauthorized person or malicious software has altered that data	Encrypted information cannot be changed except by authorized users who have the key.
Availability	Ensures that data is accessible to authorized users	Authorized users are provided the decryption key to access the information.
Authentication	Provides proof of the genuineness of the user	Proof that the sender was legitimate and not an imposter can be obtained.
Nonrepudiation	Proves that a user performed an action	Individuals are prevented from fraudulently denying that they were involved in a transaction.

Table 6-2 Information protections by cryptography

Types of Cryptography There are three broad categories of cryptographic algorithms. These are known as hash algorithms, symmetric cryptographic algorithms, and asymmetric cryptographic algorithms.

Hash Algorithms The most basic type of cryptographic algorithm is a one-way hash algorithm. A **hash** algorithm creates a unique "digital fingerprint" of a set of data and is commonly called *hashing*. This fingerprint, called a **digest** (sometimes called a *message digest* or *hash*), represents the contents. Although hashing is considered a cryptographic algorithm, its purpose is not to create ciphertext that can later be decrypted. Instead, hashing is "one-way" in that its contents cannot be used to reveal the original set of data. Hashing is used primarily for comparison purposes.

Hash algorithms are used extensively with passwords. When a password is first created by the user, a hash algorithm is used to create a digest or digital representation of that password and is stored on the computer or website. Password digests are covered in Chapter 2.

A secure hash that is created from a set of data cannot be reversed. For example, if 12 is multiplied by 34 the result is 408. If a user was asked to determine the two numbers used to create the number 408, it would not be possible to "work backward" and derive the original numbers with absolute certainty because there are too many mathematical possibilties (204 + 204, 204 × 2, 407 + 1, 102 × 4, 361 + 47, etc.). Hashing is similar in that it is used to create a value, but it is not possible to determine the original set of data.

A hashing algorithm is considered secure if it has these characteristics:

- *Fixed size.* A digest of a short set of data should produce the same size as a digest of a long set of data. For example, a digest of the single letter *a* is 86be7afa339d0fc7cfc785e72f578d33, while a digest of 1 million occurrences of the letter *a* is 4a7f5723f954eba1216c9d8f6320431f, the same length.
- *Unique.* Two different sets of data cannot produce the same digest, which is known as a *collision*. Changing a single letter in one data set should produce an entirely different digest. For example, a digest of *Sunday* is 0d716e73a2a7910bd4ae634 07056d79b, while a digest of *sunday* (lowercase *s*) is 3464eb71bd7a4377967a30-32#da798a1b54.
- *Original.* It should be impossible to produce a data set that has a desired or predefined hash.
- *Secure.* The resulting hash cannot be reversed in order to determine the original plaintext.

Hashing is often used to determine the integrity of a message or contents of a file. In this case, the digest serves as a check to verify that the original contents have not changed. For example, digest values are often posted on websites in order to verify the integrity of files that can be downloaded. A user can create a digest on a file after it has been downloaded and then compare that value with the original digest value posted on the website. A match indicates that the integrity of the file has been preserved. This is shown in Figure 6-3.

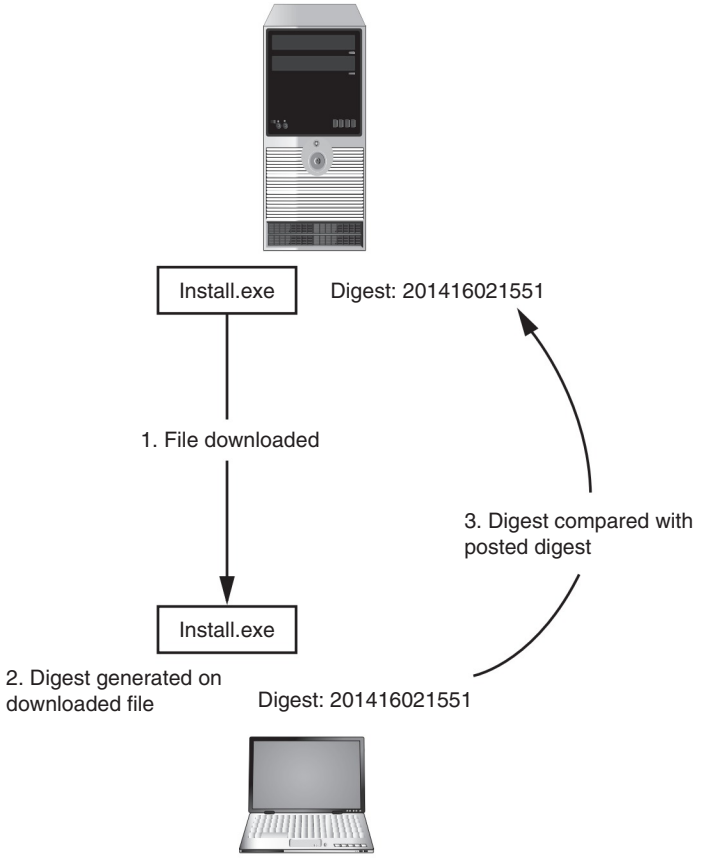


Figure 6-3 Verifying file integrity with digests

At one time, in some countries, a customer's automated teller machine (ATM) card stored the digest of the customer's personal identification number (PIN) on the back of the card. When the PIN was entered on the ATM, it was hashed and then compared with the digest stored on the back of the card. If the numbers matched, the customer's identity was verified. This prevented a thief from easily using a stolen card. These types of cards, however, are no longer used.

Symmetric Cryptographic Algorithms The original cryptographic algorithms for encrypting and decrypting data are symmetric cryptographic algorithms. **Symmetric cryptographic algorithms** use the same single key to encrypt and decrypt a document. Unlike hashing, in which the hash is not intended to be decrypted, symmetric algorithms are designed to encrypt and decrypt the ciphertext. Data encrypted with a symmetric cryptographic algorithm by Alice will be decrypted when received by Bob. It is therefore essential that the key be kept private (confidential), because if an attacker obtained the key he could read all the encrypted documents. For this reason, symmetric encryption is also called **private key**

cryptography. Symmetric encryption is illustrated in Figure 6-4 where identical keys are used to encrypt and decrypt a document. Symmetric cryptography can provide strong protections against attacks as long as the key is kept secure.

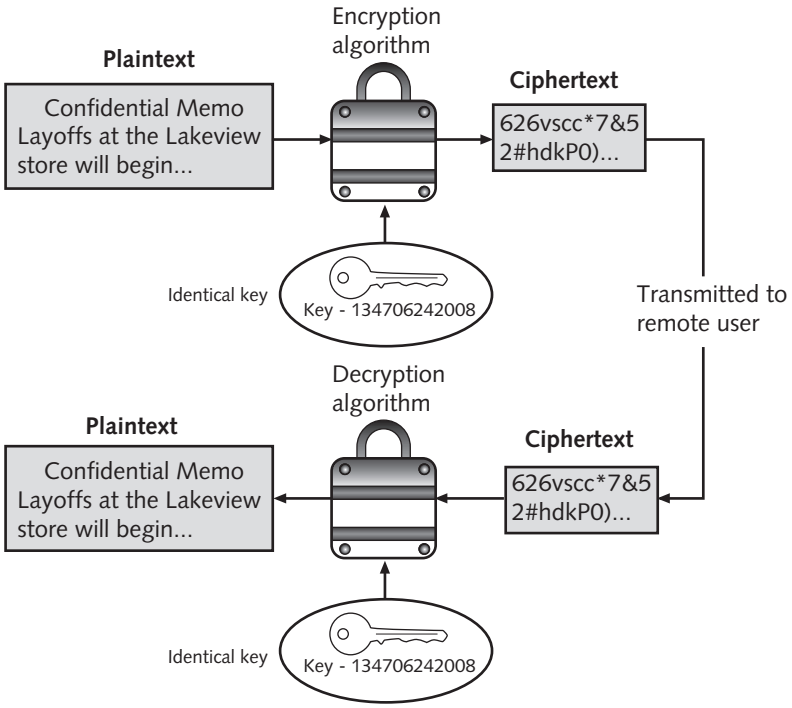


Figure 6-4 Symmetric (private key) cryptography

Asymmetric Cryptographic Algorithms If Bob wants to send an encrypted message to Alice using symmetric encryption, he must be sure that she has the key to decrypt the message. Yet how should Bob get the key to Alice? He cannot send it electronically through the Internet, because that would make it vulnerable to interception by attackers. Nor can he encrypt the key and send it, because Alice would not have a way to decrypt the encrypted key. This example illustrates the primary weakness of symmetric encryption algorithms: distributing and maintaining a secure single key among multiple users, who are often scattered geographically, poses significant challenges.

A completely different approach from symmetric cryptography is to use **asymmetric cryptographic algorithms**, also known as **public key cryptography**. Asymmetric encryption uses two keys instead of only one. These keys are mathematically related and are known as the public key and the private key. The **public key** is known to everyone and can be freely distributed, while the **private key** is known only to the individual to whom it belongs. When Bob wants to send a secure message to Alice, he uses Alice's public key to encrypt the message. Alice then uses her private key to decrypt it. Asymmetric cryptography is illustrated in Figure 6-5.

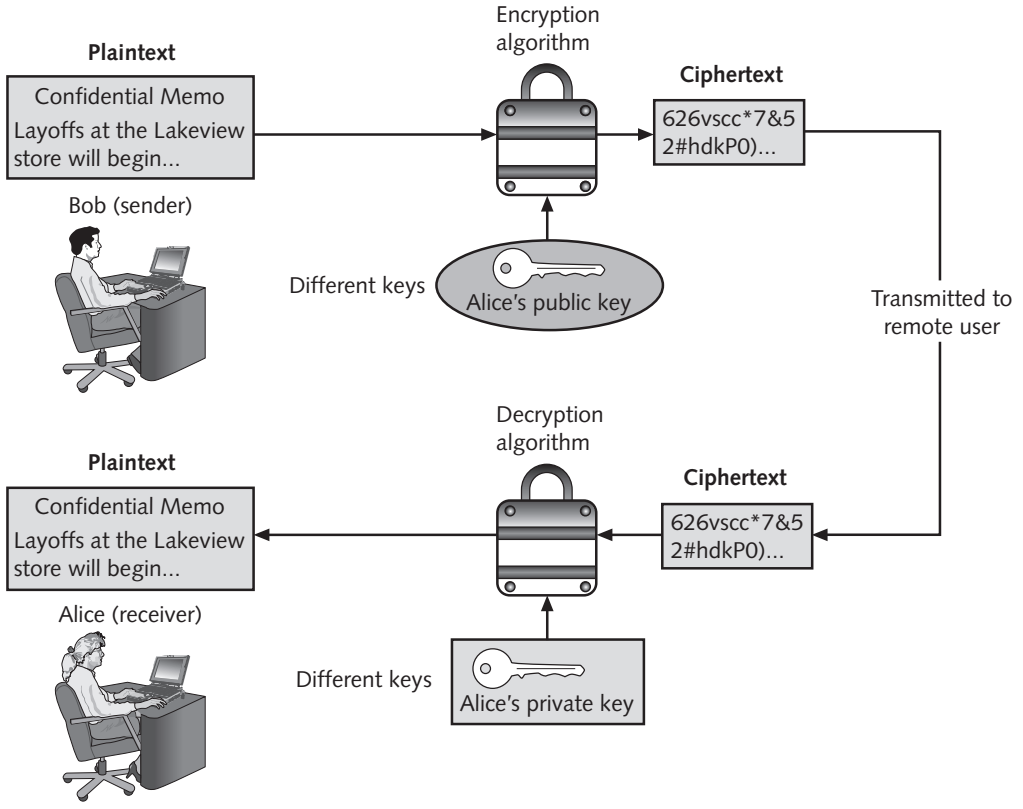


Figure 6-5 Asymmetric (public key) cryptography

Several important principles regarding asymmetric cryptography are:

- *Key pairs*. Unlike symmetric cryptography that uses only one key, asymmetric cryptography requires a pair of keys.
- *Public key*. Public keys by their nature are designed to be "public" and do not need to be protected. They can be freely given to anyone or even posted on the Internet.
- *Private key*. The private key should be kept confidential and never shared.
- *Both directions*. Asymmetric cryptography keys can work in both directions. A document encrypted with a public key can be decrypted with the corresponding private key. In the same way, a document encrypted with a private key can be decrypted with its public key.

Asymmetric cryptography also can be used to provide proof of the sender's identity and that the data has not been intercepted or altered. Suppose that Alice receives an encrypted document that says it came from Bob. Although Alice can be sure that the encrypted message was not viewed or altered by someone else while being transmitted, how can she know for certain that Bob was actually the sender? Because Alice's public key is widely available, anyone could use it to encrypt the document. Another individual could have

created a fictitious document, encrypted it with Alice's public key, and then sent it to Alice while pretending to be Bob. Alice's key can verify that no one read or changed the document in transport, but it cannot verify the sender.

Proof can be provided with asymmetric cryptography, however, by creating a **digital signature**, which is an electronic verification of the sender. A handwritten signature on a paper document serves as proof that the signer has read and agreed to the document. A digital signature is much the same but can provide additional benefits. A digital signature can:

- *Verify the sender*. A digital signature serves to confirm the identity of the person from whom the electronic message originated.
- *Prevent the sender from disowning the message*. The signer cannot later attempt to disown it by claiming the signature was forged (nonrepudiation).
- *Prove the integrity of the message*. A digital signature can prove that the message has not been altered since it was signed.

The basis for a digital signature rests on the ability of asymmetric keys to work in both directions (a public key can encrypt a document that can be decrypted with a private key, and the private key can encrypt a document that can be decrypted by the public key). The steps for Bob to send a digitally signed message to Alice are:

1. After creating a memo, Bob generates a digest on it.
2. Bob then encrypts the digest with his private key. This encrypted digest is the digital signature for the memo.
3. Bob sends both the memo and the digital signature to Alice.
4. When Alice receives them, she decrypts the digital signature using Bob's public key, revealing the digest. If she cannot decrypt the digital signature, then she knows that it did not come from Bob (because only Bob's public key is able to decrypt the digest generated with his private key).
5. Alice then hashes the memo with the same hash algorithm Bob used and compares the result to the digest she received from Bob. If they are equal, Alice can be confident that the message has not changed since he signed it. If the digests are not equal, Alice will know the message has changed since it was signed.

These steps are illustrated in Figure 6-6.

Using a digital signature does not encrypt the message itself. In the example, if Bob wanted to ensure the privacy of the message, he also would have to encrypt it using Alice's public key.

Public and private keys may result in confusion regarding whose key to use and which key should be used. Table 6-3 lists the practices to be followed when using asymmetric cryptography.

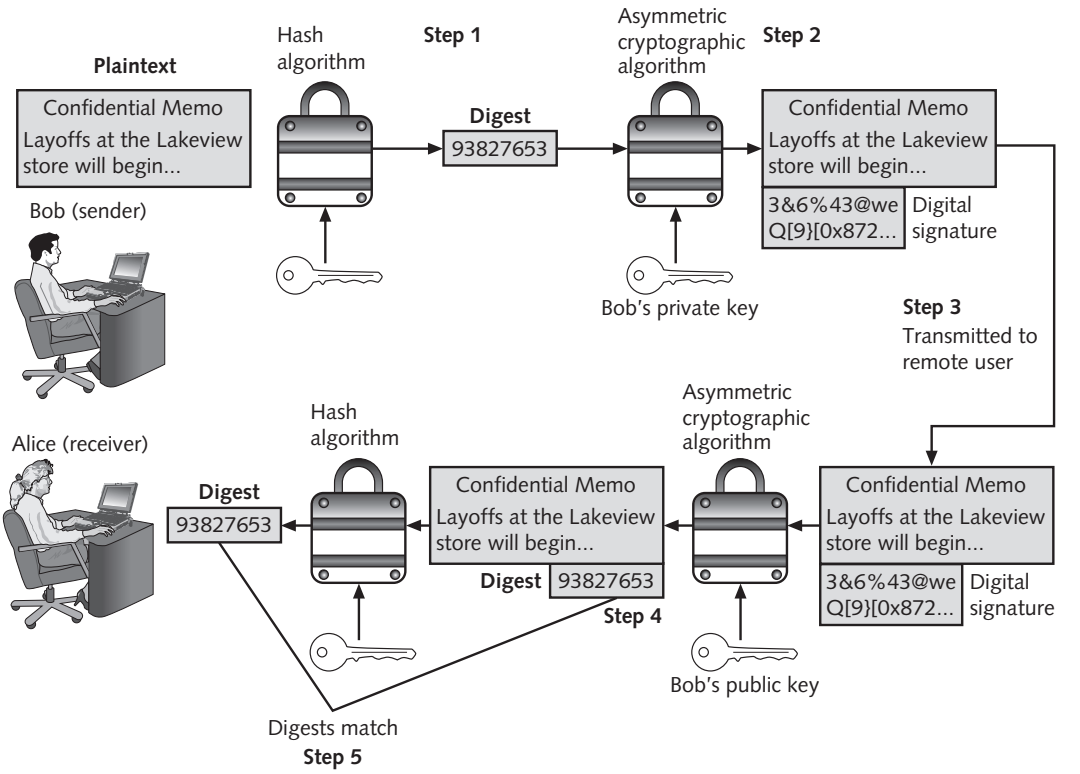


Figure 6-6 Digital signature

Action	Whose key to use	Which key to use	Explanation
Bob wants to send Alice an encrypted message	Alice's key	Public key	When an encrypted message is to be sent, the recipient's, and not the sender's, key is used.
Alice wants to read an encrypted message sent by Bob	Alice's key	Private key	An encrypted message can be read only by using the recipient's private key.
Bob wants to send a copy to himself of the encrypted message that he sent to Alice	Bob's key	Public key to encrypt Private key to decrypt	An encrypted message can be read only by the recipient's private key. Bob would need to encrypt it with his public key and then use his private key to decrypt it.
Bob receives an encrypted reply message from Alice	Bob's key	Private key	The recipient's private key is used to decrypt received messages.
Bob wants Susan to read Alice's reply message that he received	Susan's key	Public key	The message should be encrypted with Susan's key for her to decrypt and read with her private key.
Bob wants to send Alice a message with a digital signature	Bob's key	Private key	Bob's private key is used to encrypt the hash.
Alice wants to see Bob's digital signature	Bob's key	Public key	Because Bob's public and private keys work in both directions, Alice can use his public key to decrypt the hash.

Table 6-3 **Asymmetric cryptography practices**

No user other than the owner should *ever* have the private key.

Using Cryptography Cryptography should be used to secure any and all data that needs to be protected. This includes individual files, databases, removable media, or data on mobile devices. Cryptography can be applied through either software or hardware.

Encryption through Software Encryption can be implemented through cryptographic software running on a desktop computer, laptop, tablet, or smartphone. There are three different methods for encryption through software:

- *Individual files*. One means for encrypting through software is to encrypt or decrypt files one-by-one. However, this can be a cumbersome process if many files need to be encrypted.
- *File system*. Instead of protecting individual files, entire groups of files, such as all files in a specific folder, can be encrypted by taking advantage of the operating system's file system. A *file system* is a method used by operating systems to store, retrieve, and organize files.
- *Whole disk encryption*. Software encryption also can be performed on a larger scale to entire disks. This is known as *whole disk encryption* and protects all data on a hard drive. In addition to protecting individual files and folders, whole disk encryption prevents attackers from accessing data by booting from another operating system or stealing the hard drive and then placing it in another computer.

Hardware Encryption Software encryption suffers from the same fate as any application program: it can be subject to attacks to exploit its vulnerabilities. As another option, cryptography can be embedded in hardware to provide an even higher degree of security. Hardware encryption cannot be exploited like software encryption.

Many instances of private data falling into the hands of unauthorized personnel are the result of USB flash drives being lost or stolen. Although this data can be secured with software-based cryptographic application programs, vulnerabilities in these programs can open the door for attackers to access the data. As an alternative, encrypted hardware-based USB devices like flash drives can be used to prevent these types of attacks. These drives, like the Apricorn Aegis Secure Key shown in Figure 6-7, resemble standard USB flash drives, with several significant differences:

- Encrypted hardware-based USB drives will not connect to a computer until the correct password has been provided.
- All data copied to the USB flash drive is automatically encrypted.
- The external cases are designed to be tamper-resistant, so attackers cannot disassemble the drives.
- Administrators can remotely control and track activity on the devices.
- Compromised or stolen drives can be remotely disabled.

Figure 6-7 Apricorn Aegis Secure Key USB encrypted drive

Source: Apricorn Co.

One hardware-based USB encrypted drive allows administrators to remotely prohibit accessing the data on a device until it can verify its status, to lock out the user completely the next time the device connects, or even to instruct the drive to initiate a self-destruct sequence to destroy all data.

Just as an encrypted hardware-based USB flash drive will automatically encrypt any data stored on it, self-encrypting hard disk drives (HDDs) can protect all files stored on them. When the computer or other device with a self-encrypting HDD is initially powered up, the drive and the host device perform an authentication process. If the authentication process fails, the drive can be configured to simply deny any access to the drive or even perform a "cryptographic erase" on specified blocks of data (a cryptographic erase deletes the decryption keys so that all data is permanently encrypted and unreadable). This also makes it impossible to install the drive on another computer to read its contents.

Self-encrypting HDDs are commonly found in copiers and multifunction printers as well as point-of-sale systems used in government, financial, and medical environments.

Digital Certificates A **digital certificate** is a technology used to associate a user's identity to a public key and that has been "digitally signed" by a trusted third party. This third party verifies the owner and that the public key belongs to that owner. When Bob sends a message to Alice, he does not ask her to retrieve his public key from a central site; instead, Bob attaches the digital certificate to the message. When Alice receives the message with the digital certificate, she can check the signature of the trusted third party on the certificate. If the signature was signed by a party that she trusts, then Alice can safely assume that the public key contained in the digital certificate is actually from Bob. Digital certificates make it possible for Alice to verify Bob's claim that the key belongs to him and prevent an attack that impersonates the owner of the public key.

One type of digital certificate is *server digital certificates* that are often issued from a web server to a user's client computer. Server digital certificates perform two functions. First, they can ensure the authenticity of the web server. Server digital certificates enable clients connecting to the web server to examine the identity of the server's owner. A user who connects to a website that has a server digital certificate issued by a trusted third party can be confident that the data transmitted to the server is used only by the person or organization identified by the certificate.

Second, server digital certificates can ensure the authenticity of the cryptographic connection to the web server. Sensitive connections to web servers, such as when a user needs to enter a credit card number to pay for an online purchase, need to be protected. Web servers can set up secure cryptographic connections so that all transmitted data is encrypted by providing the server's public key with a digital certificate to the client. This handshake between web browser and web server is illustrated in Figure 6-8:

1. The web browser sends a message ("ClientHello") to the server that contains information including the list of cryptographic algorithms that the client supports.

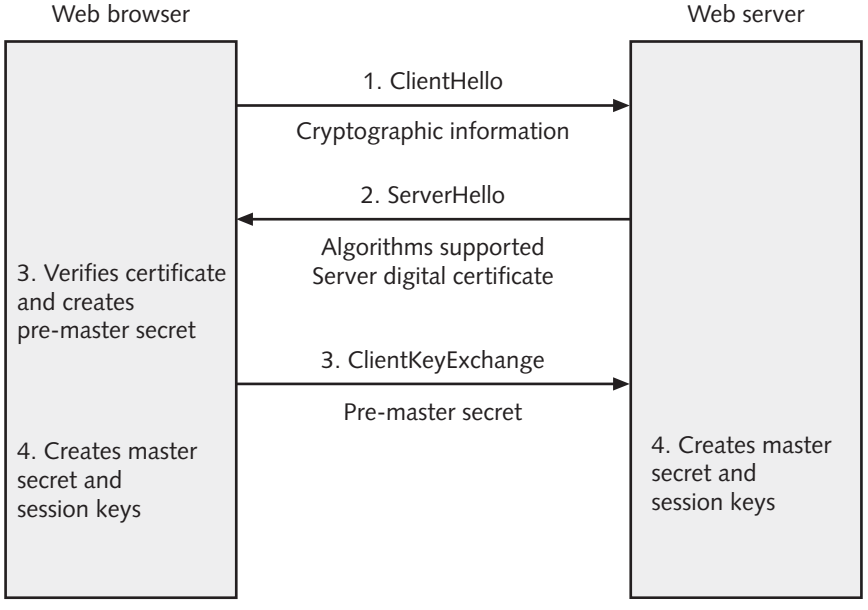


Figure 6-8 Server digital certificate handshake

2. The web server responds ("ServerHello") by indicating which cryptographic algorithm will be used. It then sends the server digital certificate to the browser.
3. The web browser verifies the server certificate (such as making sure it has not expired) and extracts the server's public key. The browser generates a random value (called the *pre-master secret*), encrypts it with the server's public key, and sends it back to the server ("ClientKeyExchange").
4. The server decrypts the message and obtains the browser's pre-master secret. Because both the browser and server now have the same pre-master secret, they can each create the same *master secret*. The master secret is used to create *session keys*, which are symmetric keys to encrypt and decrypt information exchanged during the session and to verify its integrity.

Most server digital certificates combine both server authentication and secure communication between clients and servers on the web, although these functions can be separate. A server digital certificate that both verifies the existence and identity of the organization and securely encrypts communications displays two items that the user can verify. First, the URL begins with *https://* instead of *http://*. Second, a padlock icon appears in the web browser. Clicking the padlock icon displays information about the digital certificate along with the name of the site, as shown in Figure 6-9 (Google Chrome browser).

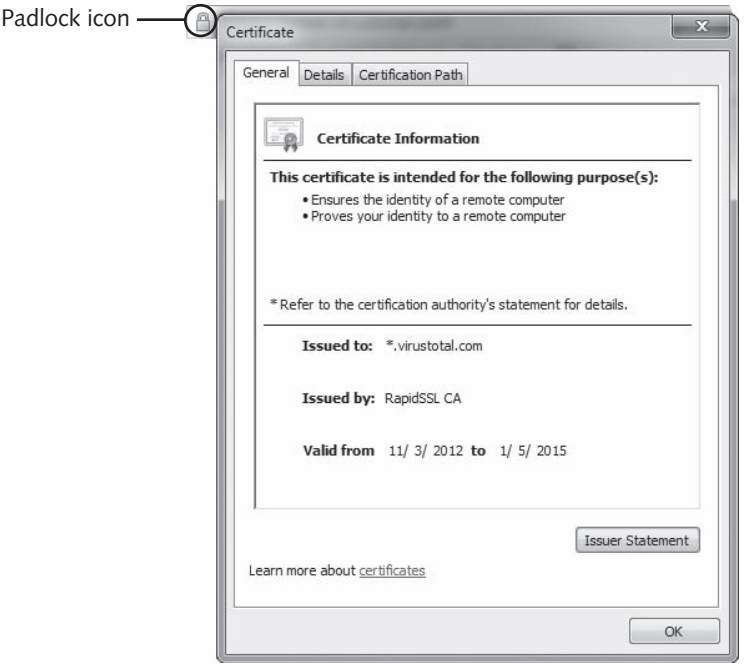


Figure 6-9 Padlock icon and certificate information

Source: Google Chrome web browser

An enhanced type of server digital certificate is the *Extended Validation SSL Certificate* (*EV SSL*). This type of certificate requires more extensive verification of the legitimacy of the business. In addition, web browsers can visually indicate to users that they are connected to a website that uses the higher-level EV SSL by using colors on the address bar.

A web browser that accesses a site that uses EV SSL displays the address bar shaded in green along with the site's name. The address bar displays in red if the site is known to be dangerous.

Privacy Best Practices

In order to protect important information users should consider the following privacy best practices:

- Use encryption to protect sensitive documents that contain personal information, such as a Social Security number, driver's license number, and bank account numbers. Store the encryption keys in a password management application.
- Be sure that strong passwords are used on all accounts that contain personal information.
- Shred financial documents and paperwork that contains personal information before discarding it.
- Do not carry a Social Security number in a wallet or write it on a check.
- Do not provide personal information either over the phone or through an email message.
- Keep personal information in a secure location in a home or apartment.
- Be cautious about what information is posted on social networking sites and who can view your information. Show "limited friends" a reduced version of a profile, such as casual acquaintances or business associates.
- Keep only the last three months of the most recent financial statements and then shred older documents instead of tossing them in the trash or a recycling bin. For paper documents that must be retained, use a scanner to create a PDF of the document and then add a strong password to the PDF file that must be entered before it can be read.
- Install antispyware software that helps prevent computers from becoming infected by spyware.
- Use a popup blocker to stop popup advertisements from appearing.
- Control cookies through the web browser. If cookies cannot be blocked, the browser should be set to delete all cookies when the browser is closed.
- Use the private browsing option available in most browsers. When not using private browsing, delete the browsing history and clear the cache after each session.
- Review the privacy options of the web browser and turn on those features that will provide the highest level of privacy without negatively impacting the browser experience.
- Turn on Wi-Fi Protected Access 2 (WPA2) Personal on Wi-Fi networks to prevent an unauthorized person from viewing wireless transmissions (see Chapter 5).
- Give cautious consideration before giving permission to a website or app request to collect data.

- Be sure that a padlock and *https* appear at the beginning of a web address that asks for credit card numbers or other sensitive information. Do not provide any information if that is not present.
- Use common sense. Websites that request more personal information than would normally be expected, such as a user name and password to another account, should be avoided.

Responsibilities of Organizations

Organizations that collect user's personal data likewise have responsibilities and obligations. These are summarized in Table 6-4 with actual examples of misuse by organizations, by the responsible action the organization should have taken, and an explanation of the practices.

Example of misuse	Responsible action	Explanation
During the online registration process the organization required new users to provide both their email address and the password to that email account, and then stored the information in cleartext.	Collect only necessary personal information.	Organizations should not collect any personal information unless it is absolutely necessary, and the information that is collected should be limited.
An organization collected customers' credit and debit card information to process transactions in its retail stores but then stored that information for 30 days, long after the sale was complete.	Keep personal information only as long as necessary.	Unless there is a legitimate business need, personal information should be securely disposed of as soon as any transactions are completed.
An organization used actual personal information in employee training sessions and then failed to remove the information from employees' computers after the training was completed.	Do not use personal information when it is not necessary.	Fictitious information should be used for any for training or development purposes.
Over 7,000 files containing users' personal information were inadvertently sent to a third party by an organization that had failed to restrict employee access to sensitive personal information.	Restrict access to sensitive information.	If employees do not need to use customers' personal information as part of their job function, access to such information should be denied.
An organization gave all of its employees administrative control over the system, including the ability to reset user account passwords and view users' comments.	Limit administrative access.	Administrative access, which allows a user to make system-wide changes, should be limited to employees who have that job function.
An organization stored sensitive customer information that was encrypted with a nonstandard and proprietary form of encryption, which contained several vulnerabilities.	Use industry-tested and accepted methods.	Organizations should take advantage of the "collected wisdom" of encryption algorithms that have been tested by experts over many years.
Sensitive personal information was thrown away in dumpsters, and hard drives that contained personal information were sold as surplus.	Dispose of sensitive data securely.	When paperwork or equipment containing personal information is no longer needed, it should be destroyed by shredding, burning, or pulverizing to make the data unreadable.

Table 6-4 Privacy responsibilities of organizations

Exceptional Security

RESTRICT YOUR INFORMATION—Decide what information about you is personal and needs to be protected. Then do not share this information, even when asked. If information absolutely must be provided, use fictitious information. If given the option, do not sign up for a new service using your Facebook account. Review and set the privacy settings for every online service you use, and revisit those policies regularly to update them, since the services tend to change their policies frequently and without warning. Do not post photos of your children or relatives, your interests, or when you will be going on vacation on social networking sites. Opt out of mail and email direct marketing. Use the Federal Trade Commission's *Do Not Call Registry* to opt out of telemarketer calls and report any violators.

PRIVATELY SURF THE WEB—Create a personal and professional online profile for browsing the web, and then use different web browsers for each persona; that is, use one browser for accessing your social media accounts and another for your professional online activities. Block all cookies. Turn on the *Do Not Track* option found on browsers. Use a secure browser that has strict built-in privacy controls. Use a search engine that does not retain your search history, or use a proxy search service that resides between your browser and the popular search engines so that your search history cannot be tracked. Use *https://* instead of *http://* whenever possible. Sign up for a virtual private network (VPN) service. Create a "disposable" webmail account that is different from your normal account and provide it when asked to give an email address. Consider creating the webmail account using an international provider that is beyond the reach of the U.S. Patriot Act to make your data less prone to government access. Also create an online phone number that you give on demand. Delete all unused online accounts.

MANAGE YOUR MOBILE DEVICES—Use a self-destructing texting and chatting service so that no information is retained. Check with your mobile phone carrier to determine options that let you limit how it uses and shares your data. Use a strong password to protect your smartphones, tablets, and mobile devices. Configure the *Find Me* feature or app for mobile devices in the event that they are lost or stolen. Use a password management application on your smartphone. Turn on two-factor authentication. Do not share your mobile location information. Completely turn off Wi-Fi and Bluetooth to avoid retail tracking when shopping.

GO EXTREME—Use only cash or disposable credit card numbers when making purchases. Check your credit report every four months, rotating through the three different report providers. Put a permanent security freeze on your credit report so that no one can access it to open up new credit accounts in your name without your permission. Use a service to monitor the information that is about you on the Internet on public online databases and delete as much as possible.

Chapter Summary

- Privacy is defined as the state or condition of being free from public attention to the degree that you determine, or the right to be left alone to the level that you choose. Prior to the current age of technology, individuals were generally able to choose the level of privacy that they desired. Today that is no longer possible, for data is collected on almost all actions and transactions that individuals perform. There are several risks associated with the use of private data.
- Cryptography is the science of transforming information into a secure form so that unauthorized persons cannot access it. Unlike steganography, which hides the existence of data, cryptography masks the content of documents or messages so that they cannot be read or altered. The original data, called plaintext, is input into a cryptographic encryption algorithm that has a mathematical value (a key) used to create ciphertext. Because access to the key can be restricted, cryptography can provide confidentiality, integrity, availability, authenticity, and nonrepudiation.
- Hashing creates a unique digital fingerprint called a digest that represents the contents of the original material. Hashing is not designed for encrypting material that will be later decrypted; it is used only for comparison. If a hash algorithm produces a fixed-size hash that is unique, and the original contents of the material cannot be determined from the hash, the hash is considered secure. Symmetric cryptography, also called private key cryptography, uses a single key to encrypt and decrypt a message. Symmetric cryptographic algorithms are designed to decrypt the ciphertext. Symmetric cryptography can provide strong protections against attacks as long as the key is kept secure. Asymmetric cryptography, also known as public key cryptography, uses two keys instead of one. These keys are mathematically related and are known as the public key and the private key. The public key is widely available and can be freely distributed, while the private key is known only to the recipient of the message and must be kept secure. Asymmetric cryptography also can be used to create a digital signature, which verifies the sender, proves the integrity of the message, and prevents the sender from disowning the message.
- Cryptography can be applied through either software or hardware. Software-based cryptography can protect individual files, groups of files, or an entire disk. Hardware encryption cannot be exploited like software cryptography. Hardware encryption devices can protect USB devices and standard hard drives.
- There are several practical best practices that users should consider when attempting to protect their personal information. In addition, organizations that collect user's personal data have responsibilities and obligations.

Key Terms

Definitions for key terms can be found in the Glossary for this text.

algorithm
asymmetric cryptographic algorithm
ciphertext
cleartext
cryptography
data broker
decryption
digital certificate

digest
digital signature
encryption
hash
key
nonrepudiation
plaintext
privacy
private key
private key cryptography
public key
public key cryptography
steganography
symmetric cryptographic algorithm

Review Questions

1. Each of the following is true about privacy EXCEPT:
   a. Privacy is the right to be left alone to the degree that you choose.
   b. Today individuals can achieve any level of privacy that is desired.
   c. Privacy is difficult due to the volume of data silently accumulated by technology.
   d. Privacy is freedom from attention, observation, or interference based on your decision.
2. Which of the following is not a risk associated with the use of private data?
   a. individual inconveniences and identity theft
   b. devices being infected with malware
   c. associations with groups
   d. statistical inferences
3. Which of the following is not an issue raised regarding how private data is gathered and used?
   a. The data is gathered and kept in secret.
   b. The accuracy of the data cannot be verified.
   c. By law, all encrypted data must contain a "backdoor" entry point.
   d. Informed consent is usually missing or is misunderstood.
4. _____ hides the existence of the data.
   a. Cryptography
   b. Symmetric encryption
   c. Asymmetric decryption
   d. Steganography
5. What is ciphertext?
   a. Procedures based on a mathematical formula used to encrypt and decrypt data.
   b. A mathematical value entered into an algorithm.
   c. Encrypted data.
   d. The public key of a symmetric cryptographic process.

6. Which of the following is "one-way" so that its contents cannot be used to reveal the original set of data?
   a. hash
   b. symmetric cryptography
   c. Message Digest Encryption (MDE)
   d. asymmetric cryptography
7. What is data called that is to be encrypted by inputting it into a cryptographic algorithm?
   a. ciphertext
   b. plaintext
   c. cleartext
   d. opentext
8. Which of these is NOT a basic security protection for information that cryptography can provide?
   a. risk loss
   b. authenticity
   c. integrity
   d. confidentiality
9. The areas of a file in which steganography can hide data include all of the following EXCEPT _____.
   a. data that is used to describe the content or structure of the actual data
   b. the directory structure of the file system
   c. the file header fields that describe the file
   d. areas that contain the content data itself
10. Proving that a user sent an email message is known as _____.
    a. repudiation
    b. integrity
    c. nonrepudiation
    d. availability
11. A(n) _____ is not decrypted but is only used for comparison purposes.
    a. stream
    b. digest
    c. algorithm
    d. key

12. Which of these is NOT a characteristic of a secure hash algorithm?
    a. A message cannot be produced from a predefined hash.
    b. Collisions should be rare.
    c. The results of a hash function should not be reversed.
    d. The hash should always be the same fixed size.
13. How many keys are used in asymmetric cryptography?
    a. one
    b. two
    c. three
    d. four
14. Which of these is not a method for encryption through software?
    a. encrypt individual files
    b. whole disk encryption
    c. encrypt using the file system
    d. encrypt using a separate hardware computer chip
15. If Bob wants to send a secure message to Alice using an asymmetric cryptographic algorithm, which key does he use to encrypt the message?
    a. Alice's private key
    b. Alice's public key
    c. Bob's public key
    d. Bob's private key
16. A digital signature can provide each of the following benefits EXCEPT _____.
    a. proving the integrity of the message
    b. verifying the receiver
    c. verifying the sender
    d. enforcing nonrepudiation
17. What is the most important advantage of hardware encryption over software encryption?
    a. Software encryption cannot be used on older computers.
    b. Hardware encryption is up to 10 times faster than software encryption.
    c. Software that performs encryption can be subject to attacks.
    d. There are no advantages of hardware encryption over software encryption.

18. Which of the following appears in the web browser when you are connected to a secure website that is using a digital certificate?
    a. *http://*
    b. wrench
    c. padlock
    d. a yellow warning message
19. Which of the following is NOT a privacy best practice?
    a. Use the private browsing option in your web browser.
    b. Shred financial documents and paperwork that contains personal information before discarding it.
    c. Use strong passwords on all accounts that contain personal information.
    d. Carry your Social Security number with you so that it cannot be stolen you are not home.
20. Each of these is a responsibility of an organization regarding user private data EXCEPT:
    a. Collect only necessary personal information.
    b. Use industry-tested and accepted methods.
    c. Keep personal information for no longer than 365 days.
    d. Do not use personal information when it is not necessary.

Hands-On Projects

Project 6-1: Using OpenPuff Steganography

Unlike cryptography that scrambles a message so that it cannot be viewed, steganography hides the existence of the data. In this project, you will use OpenPuff to create a hidden message.

1. Use your web browser to go to **embeddedsw.net/OpenPuff_Steganography_ Home.html** (if you are no longer able to access the site through the web address, use a search engine to search for "OpenPuff").
2. Click **Source Page** and then click **Manual** to open the OpenPuff manual. Save this file to your computer. Read through the manual to see the different features available.
3. Click your browser's back button to return to the home page.
4. Click **OpenPuff** to download the program.
5. Navigate to the location of the download and uncompress the Zip file on your computer.
6. Now create a carrier file that will contain the hidden message. Open a Windows search box and enter **Snipping Tool**.

For added security, OpenPuff allows a message to be spread across several carrier files.

7. Launch **Snipping Tool**.
8. Click the **New** menu arrow, then click **Window Snip**.
9. Capture the image of one of the pages of the OpenPuff manual. Click **File** and **Save As**. Enter **Carrier1.png** and save to a location such as the desktop.
10. Now create the secret message to be hidden. Create a new Word file and enter **This is a secret message**.
11. Save this file as **Message.docx**.
12. Exit Word.
13. Create a Zip file from **Message**. Navigate to the location of this file through Windows Explorer and click the right mouse button.
14. Click **Send to** and select **Compressed (zipped) folder** to create the Zip file.
15. Navigate to the OpenPuff directory and double-click **OpenPuff.exe**.
16. Click **Hide** in the **Steganography** section.

Under Bit selection options, note the wide variety of file types that can be used to hide a message.

17. Under (**1**), create three unrelated passwords and enter them into **Cryptography** (**A**), (**B**), and (**C**).
18. Under (**2**), locate the message to be hidden. Click **Browse** and navigate to the file **Message.zip**. Click **Open**.
19. Under (**3**), select the carrier file. Click **Add** and navigate to **Carrier1.png** and click **Open** as shown in Figure 6-10.
20. Click **Hide Data!**
21. Navigate to a different location than that of the carrier files and click **OK**. Click **Done** in the **Task Report** window.
22. After the processing is completed, navigate to the location of the carrier file that contains the message and open the file. Can you detect anything different with the file now that it contains the message?
23. Now uncover the message. Close the OpenPuff Data Hiding screen to return to the main menu.
24. Click **Unhide**.

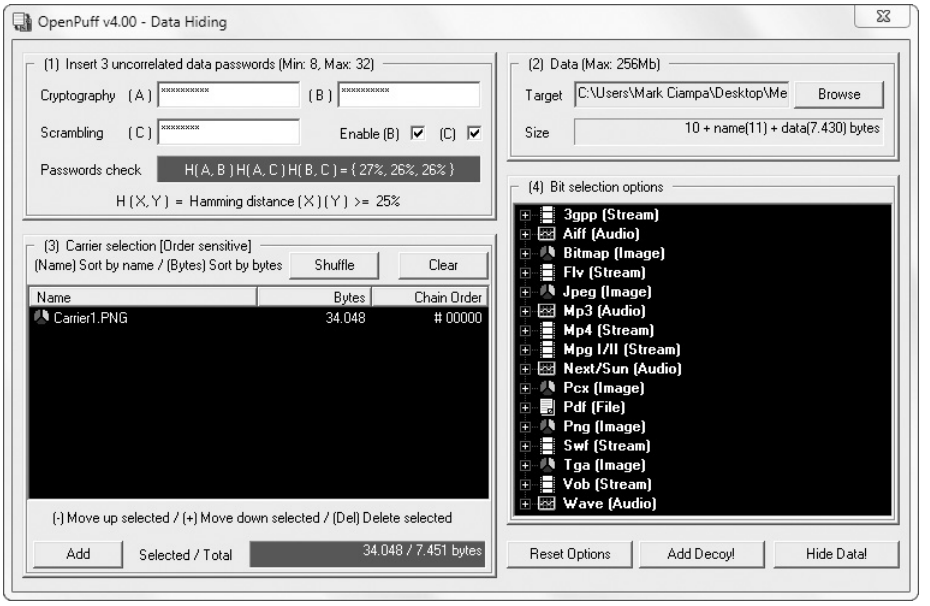


Figure 6-10 OpenPuff

Source: EmbeddedSW.net

25. Enter the three passwords.
26. Click **Add Carriers** and navigate to the location of **Carrier1** that contains the hidden message and click **Open**.
27. Click **Unhide!** and navigate to a location to deposit the hidden message. When it has finished processing click **OK**.
28. Click **Done** after reading the report.
29. Go to that location and you will see **Message.zip**.
30. Close OpenPuff and close all windows.

Project 6-2: Viewing Digital Certificates

In this project, you will view digital certificate information using a Google Chrome web browser.

1. Use your web browser to go to **www.google.com.**
2. Note that although you did not enter *https://*, nevertheless Google created a secure connection. Why would it do that? What are the advantages?
3. Click the padlock icon in the browser address bar.
4. In the **Permissions** tab, under **Cookies and site data,** how many cookies are allowed from this site? Why?

5. Under **Permissions,** are there any permissions that have been restricted?
6. Click the **Connection** tab.
7. Read the information about the identity of this website.
8. Click the **Certificate information** link.
9. Note the general information displayed under the **General** tab.
10. Now click the **Details** tab.
11. Click **Valid to** to view the expiration date of this certificate.
12. Click **Public key** to view the public key associated with this digital certificate. Why is this site not concerned with distributing this key? How does embedding the public key in a digital certificate protect it from impersonators?
13. Click the **Certification Path** tab. Because web certificates are based on the distributed trust model, there is a "path" to the root certificate. Click the root certificate and click the **View Certificate** button. Click the **Details tab** and then click **Valid to**. Notice that the expiration date of this root certificate (belonging to the third-party verifier) is longer than that of the website certificate (provided to the website). Click **OK** and then click **OK** again to close the Certificate window.
14. Now go to a website from which you have purchased items online. Does it default to *https://*? If not, then enter your account information to log into this site.
15. Click the padlock icon in the browser address bar and view the information about this certificate as you did above.
16. How would you explain the purpose of digital certificates to a friend? Is it easy to show someone how to determine if the certificate is valid? How could this be improved?
17. Close all windows.

Project 6-3: Installing Hash Generator and Comparing Digests

In this project, you will download a hash generator and compare the results of various hash algorithms.

1. Create a Microsoft Word document with the contents **Now is the time for all good men to come to the aid of their country**.
2. Save the document as **CountryWithDot.docx**.
3. Now remove the period at the end of the sentence and save the document as **CountryWithoutDot.docx**. Close the file.
4. Use your web browser to go to **implbits.com/products/hashtab** (if you are no longer able to access the site through the web address, use a search engine to search for "Hashtab").
5. Click **Download Now!**

6. Enter an email address to receive a direct link to download the file and click **Send Download Link**.
7. Follow the default instructions to install Hash Tab.
8. Navigate to the document **CountryWithDot.docx**.
9. Click once on **CountryWithDot.docx** and then right-click.
10. Click **Properties**.
11. Notice that there is a new tab, **File Hashes**. Click this tab to display the digests for this file.
12. Click **Settings**.
13. Click the **Select All** button.
14. Click **OK**.
15. Scroll through the different digests generated.
16. Click **Compare a file**.
17. Navigate to the file **CountryWithoutDot.docx** and then click **Open**.
18. A digest is generated on this file. What tells you that the digests are not the same? Note that the only difference between the two files is a single period. How different are the digests based on a single period?
19. Close all windows.

Project 6-4: Using a Secure Email Addition

Basic email lacks many privacy features. However, additions are available that allow users to encrypt and control emails. In this project, you will download and install a secure email addition to a Google Gmail account.

1. Use your Google Chrome web browser to go to **criptext.com** (if you are no longer able to access the site through the web address, use a search engine to search for "Criptext").
2. Click **Install on Gmail**.
3. Click **Add extension**.
4. After the extension is added, your Gmail account will launch. Click **Activate Now**.
5. Click the **Allow** button in the **Request for Permission** box.
6. Click **Compose** to create a new email message.
7. Click the **Enable** box to turn on Criptext.
8. Send an email message to another email account.
9. Click **Send Securely** to encrypt the email and send it.
10. Access the second email account and read the message.

11. Click the **Email Activity** button in Gmail. What does it show?
12. Now recall the message. Click the **UNSEND** button next to this message. What happens to the message?
13. Click **Compose** to send another message. Create an email message but this time click the timer icon. When the **Set expiration time** dialog box appears, set the time at **1 minute**. Click **Set**.
14. Click **Send Securely**.
15. When the email arrives, open it and read the message.
16. After one minute, what happens to the email message?
17. Close all windows.

Case Projects

Case Project 6-1: Microsoft Windows 10 Privacy

With the introduction of Microsoft Windows 10, Microsoft by default gathers information about user preferences. For example, Windows 10 assigns an advertising ID to users and then uses it to deliver customized ads and information. This has caused alarm among some users regarding intrusion into their privacy. Using the Internet, research the information gathered through Windows 10. What are the advantages of this data collection? What are the disadvantages? Is this any different from how other operating systems and websites gather information? Should Microsoft be more upfront about the collection of this data? Is there a way to turn the data collection off? If so, how is it done? Should it be easier to turn it off for users who do not want their data collected? Write a one-page paper on your research and opinions.

Case Project 6-2: Information Security Community Site Activity

The Information Security Community Site is an online companion to this textbook. It contains a wide variety of tools, information, discussion boards, and other features to assist learners. Go to *community.cengage.com/infosec*. Sign in with the login name and password that you created in Chapter 1.

How do you feel about the NSA gathering data on American citizens? Is it a serious intrusion on privacy? Or is it a practical protection in the world today in order to keep the nation safe? Should there be laws in place to prevent this? Record your responses on the Community Site discussion board.

Additional Case Projects for this chapter are available through the MindTap online learning environment.

References

1. Tucker, Patrick, "Has Big Data Made Anonymity Impossible?", *MIT Technical Review*, May 7, 2013, accessed Sep. 12, 2015. http://www.technologyreview.com/news/514351/has-big-data-made-anonymity-impossible/.
2. Hardesty, Larry, "Privacy Challenges," *MIT News*, Jan. 29, 2015, accessed Sep. 12, 2015. http://news.mit.edu/2015/identify-from-credit-card-metadata-0129.
3. Halliday, Josh, "Facebook Users Unwittingly Revealing Intimate Secrets, Study Finds," *The Guardian*, Mar. 11, 2013, accessed Sep. 12, 2015. http://www.theguardian.com/technology/2013/mar/11/facebook-users-reveal-intimate-secrets.
4. Dixson, Pam and Gellman, Robert, "The Scoring of America: How Secret Consumer Scores Threaten Your Privacy and Your Future," *World Privacy Forum*, Apr. 2, 2014, accessed Sep. 12, 2015. http://www.worldprivacyforum.org/wp-content/uploads/2014/04/WPF_Scoring_of_America_April2014_fs.pdf.
5. Madden, Mary, "Public Perceptions of Privacy and Security in the Post-Snowden Era," *Pew Research Center*, Nov. 12, 2014, accessed Sep. 12, 2015. http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/.

Glossary

access point (AP) A more sophisticated device used in an office setting instead of a wireless router.

accounting The ability that provides tracking of events.

add-on Web browser addition that adds functionality to the entire web browser.

adware A software program that delivers advertising content in a manner that is unexpected and unwanted by the user.

algorithm Procedures based on a mathematical formula used to encrypt and decrypt the data.

Android The Google operating system for mobile devices that is not proprietary but is entirely open for anyone to use or even modify.

antispyware Software that that helps prevent computers from becoming infected by different types of spyware.

antivirus (AV) Software that examines a computer for any infections as well as monitors computer activity and scans new documents that might contain a virus.

arbitrary code execution A malware payload that allows an attacker to execute virtually any command on the victim's computer.

asset An item that has value.

asymmetric cryptographic algorithm Cryptography that uses two mathematically related keys.

attachment File, such as a word processing document, spreadsheet, or picture, that is attached to an email message.

authentication The steps that ensure that the individual is who he or she claims to be; the process of providing proof of genuineness.

authorization The act of providing permission or approval to technology resources.

availability Security actions that ensure that data is accessible to authorized users.

backdoor Software code that gives access to a program or a service that circumvents normal security protections.

blacklist A list of senders from whom the user does not want to receive any email.

bluejacking An attack that sends unsolicited messages to Bluetooth-enabled devices.

bluesnarfing An attack that accesses unauthorized information from a wireless device through a Bluetooth connection.

Bluetooth A short-range wireless technology designed for quickly interconnecting devices.

bot herder An attacker who controls a botnet.

botnet A logical computer network of zombies under the control of an attacker.

broker Attacker who sells knowledge of a vulnerability to other attackers or governments.

browser A program for displaying webpages.

brute force attack A password attack in which every possible combination of letters, numbers, and characters is used to match passwords in a stolen password file.

ciphertext Data that has been encrypted.

cleartext Unencrypted data.

computer virus (virus) Malicious computer code that, like its biological counterpart, reproduces itself on the same computer.

confidentiality Security actions that ensure that only authorized parties can view the information.

cookie A file created by a web server and stored on the local computer that contains the user's preferences and other information.

cryptography The science of transforming information into a secure form so that unauthorized persons cannot access it.

cybercrime Targeted attacks against financial networks, unauthorized access to information, and the theft of personal information.

cybercriminal Individual who participates in a network of attackers, identity thieves, spammers, and financial fraudsters.

cyberterrorism A premeditated, politically motivated attack against information, computer systems, computer programs, and data, which often results in violence.

cyberterrorist Attacker whose motivation may be defined as ideological, or attacking for the sake of principles or beliefs.

data backup A copy of files from a computer's hard drive saved on other digital media that is stored in a secure location.

data broker Organization that aggregates user data and then sells it to interested third parties.

decryption The process of changing ciphertext into plaintext.

dictionary attack A password attack that compares common dictionary words against those in a stolen password file.

digest The unique digital fingerprint created by a one-way hash algorithm.

digital certificate A technology used to associate a user's identity to a public key and that has been "digitally signed" by a trusted third party.

digital signature An electronic verification of the sender.

drive-by download An attack that results from a user visiting a specially crafted malicious webpage.

dumpster diving Digging through trash receptacles to find information that can be useful in an attack.

embedded hyperlink Link contained within the body of the message as a shortcut to a website.

encryption The process of changing plaintext into ciphertext.

evil twin An AP or another computer that is set up by an attacker designed to mimic the authorized Wi-Fi device.

exploit kit Automated attack package that can be used without an advanced knowledge of computers.

extension Web browser addition that expands the normal capabilities of a web browser for a specific webpage.

Fair and Accurate Credit Transactions Act (FACTA) of 2003 A U.S. law that contains rules regarding consumer privacy.

feature update Enhancements to the software to provide new or expanded functionality, but do not address security vulnerability.

firewall Hardware or software designed to limit the spread of malware.

first-party cookie A cookie that is created from the website that a user is currently viewing.

Gramm-Leach-Bliley Act (GLBA) A U.S. law that requires banks and financial institutions to alert customers of their policies and practices in disclosing customer information.

hactivist Attacker who attacks for ideological reasons that are generally not as well defined as a cyberterrorist's motivation.

hash An algorithm that creates a unique digital fingerprint.

Health Insurance Portability and Accountability Act (HIPAA) A U.S. law designed to guard protected health information and implement policies and procedures to safeguard it.

hoax A false warning intended to trick a user into performing an action that will compromise security.

HTML5 The most recent version of HTML that standardizes sound and video formats.

Hypertext Markup Language (HTML) A language that allows web authors to combine text, graphic images, audio, and video into a single document.

Hypertext Transfer Protocol (HTTP) A subset of a larger set of standards for Internet transmission.

identity theft Stealing another person's personal information, such as a Social Security number, and then using the information to impersonate the victim, generally for financial gain.

image spam Spam that uses graphical images of text in order to circumvent text-based filters.

IMAP (Internet Mail Access Protocol) A more recent and advanced email protocol.

information security The tasks of protecting the integrity, confidentiality, and availability of information on the devices that store, manipulate, and transmit the information through products, people, and procedures.

insiders Employees, contractors, and business partners who can be responsible for an attack.

Institute of Electrical and Electronics Engineers (IEEE) The most widely known and influential organization in the field of computer networking and wireless communications. The IEEE sets wireless networking standards.

integrity Security actions that ensure that the information is correct and no unauthorized person or malicious software has altered the data.

Internet A global network that allows devices connected to it to exchange information.

iOS The operating system developed by Apple for its mobile devices, using a closed and proprietary architecture.

jailbreaking Removing the built-in limitations and protections on Apple iOS devices.

Java A complete programming language that can be used to create stand-alone applications.

JavaScript A popular scripting code that is embedded within HTML documents.

key A mathematical value entered into a cryptographic algorithm to produce encrypted data.

keylogger Software or a hardware device that captures and stores each keystroke that a user types on the computer's keyboard.

locally shared object (LSO) A special type of cookie that can store more complex data, also called a *Flash cookie*.

location services Services that can identify the location of a person carrying a mobile device, or a specific store or restaurant.

lock screen Technology that prevents a mobile device from being used until the user enters the correct passcode, such as a PIN, password, swipe pattern on the screen, or a fingerprint touch ID.

logic bomb Computer code that lies dormant until it is triggered by a specific logical event.

malvertising Attacks that are based on malicious code sent through third-party advertising networks so that malware is distributed through ads sent to users' web browsers.

malware Software that enters a computer system without the user's knowledge or consent and then performs an unwanted and usually harmful action.

network firewall A hardware device that is located at the "edge" of the network as the first line of defense defending the network and devices connected to it.

nonrepudiation The process of proving that a user performed an action.

password A secret combination of letters, numbers, and/or symbols that serves to authenticate a user by what he or she knows.

password manager One of several types of tools for securing passwords, including password generators, online vaults, and password management applications.

patch A publicly released software security update intended to repair a vulnerability.

Payment Card Industry Data Security Standard (PCI DSS) A set of security standards that all U.S. companies processing, storing, or transmitting credit card information must follow.

personal firewall Software that runs as a program on the local computer to block or filter traffic coming into and out of the computer.

phishing Sending an email or displaying a web announcement that falsely claims to be from a legitimate enterprise in an attempt to trick the user into surrendering private information.

plaintext Cleartext data that is to be encrypted and decrypted by a cryptographic algorithm.

plug-in A web browser addition that adds new functionality to the web browser so that users can play music, view videos, or display special graphical images within the browser that normally it could not play or display.

popup blocker A separate program or a feature incorporated within a browser that stops popup advertisements from appearing.

Post Office Protocol (POP) An earlier email protocol for handling incoming mail.

pretexting Creating an invented scenario to persuade the victim to perform an action or provide confidential information.

privacy The state or condition of being free from public attention to the degree that the user chooses.

private key An asymmetric encryption key that does have to be protected.

private key cryptography Cryptographic algorithms that use a single key to encrypt and decrypt a message.

Protected View A Microsoft Office function that automatically opens documents attached to emails in a read-only mode that disables editing functions.

public key An asymmetric encryption key that does not have to be protected.

public key cryptography Cryptography that uses two mathematically related keys.

ransomware Malware that prevents a user's device from properly operating until a fee is paid.

reading pane An email client feature that allows the user to read an email message without actually opening it.

remote code execution Malware that can trigger arbitrary code execution from one computer to a second computer over a network or the Internet.

remote wiping The ability to remotely erase data stored on a mobile device.

risk A situation that involves exposure to danger.

rooting Removing the built-in limitations and protections on Google Android devices.

rootkit A set of software tools used by an attacker to hide the actions or presence of other types of malicious software.

Sarbanes-Oxley Act (Sarbox) A U.S. law designed to fight corporate corruption.

script kiddie Individual who lacks advanced knowledge of computers and networks and so

uses downloaded automated attack software to attack information systems.

service pack Software that is a cumulative package of all patches and feature updates.

shoulder surfing Viewing information that is entered by another person.

sideloading Downloading an app from an unofficial third-party website.

signature file A database of viruses that is used to identify an infected file.

Simple Mail Transfer Protocol (SMTP) An earlier protocol for email that handles outgoing mail.

smartphone A cellular phone that has an operating system that allows it to run apps and access the Internet.

social engineering A means of gathering information for an attack by relying on the weaknesses of individuals.

social networking Grouping individuals and organizations into clusters based on an affiliation.

spam Unsolicited email.

spam filter Software that inspects email messages to identify and stop spam.

spear phishing A phishing attack that targets only specific users.

spyware A general term used to describe software that spies on users by gathering information without consent.

state-sponsored attacker Attacker commissioned by governments to attack enemies' information.

steganography Hiding the existence of data within another type of file.

strong password A long and complex password.

symmetric cryptographic algorithm Encryption that uses a single key to encrypt and decrypt a message.

tablet Portable computing device that is generally larger than a smartphone and smaller than a laptop, and is focused on ease of use.

third-party cookie A cookie that is created by a third party other than the main website that is being viewed.

threat A type of action that has the potential to cause harm.

threat agent A person or element that has the power to carry out a threat.

threat likelihood The probability that a threat will actually occur.

threat vector The means by which an attack could occur.

Transmission Control Protocol/Internet Protocol (TCP/IP) The standards for Internet transmissions.

Trojan horse (Trojan) An executable program that is advertised as performing one activity but which actually performs a malicious activity.

typo squatting Redirecting a user to a fictitious website based on a misspelling of the URL.

User Account Control (UAC) A Microsoft Windows function that provides information to users and obtains their approval before a program can make a change to the computer's settings.

username A unique name used for identification in a computer system or website.

virtual private network (VPN) A technology that uses an unsecured public network, such as the Internet, as if it were a secure private network, by encrypting data transmissions.

vishing A phishing attack in which the attacker calls the victim on the telephone.

vulnerability A flaw or weakness that allows a threat agent to bypass security.

war driving Searching for wireless signals from an automobile or on foot using a portable computing device.

weak password A password that can easily be broken and compromises security.

wearable technology A new class of mobile technology consisting of devices that can be worn by the user instead of carried.

whaling A phishing attack that targets wealthy individuals, who typically would have larger sums of money in a bank account that an attacker could access.

whitelist A list of senders from whom the user will accept email.

Wi-Fi (wireless fidelity) A wireless data network that is designed to provide high-speed data connections for mobile devices.

Wi-Fi Protected Access 2 (WPA2) Personal A security setting that provides the optimum level of wireless security.

Wi-Fi Protected Setup (WPS) A simplified and optional method for configuring WPA2 Personal wireless security, but has security weaknesses.

wireless client network interface card adapter A device that allows a mobile device to send and receive wireless signals.

wireless local area network (WLAN) The technical name for a Wi-Fi network.

wireless router A device used for a home-based Wi-Fi network that combines several networking technologies.

World Wide Web (WWW) A network composed of Internet server computers on networks that provide online information in a specific format, commonly known as *the web*.

worm A malicious program designed to enter a computer via a network to take advantage of a vulnerability in an application or an operating system.

zombie An infected computer that is under the remote control of an attacker.

Index

D

E

F

G

H

I

J

K

L

Q

R

S

T

U

V

W

Z